

VMware Cloud Foundation 3.9.1 Site Protection and Recovery

10 MAR 2020

VMware Validated Design

VMware Cloud Foundation 3.9.1



vmware®

You can find the most up-to-date technical documentation on the VMware website at:

<https://docs.vmware.com/>

If you have comments about this documentation, submit your feedback to

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Copyright © 2018-2020 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

Contents

About VMware Cloud Foundation 3.9.1 Site Protection and Recovery	7
1 Failover and Failback Checklist for the SDDC Management Applications for VMware Cloud Foundation	9
2 Prerequisites for Implementing Disaster Recovery on VMware Cloud Foundation	11
3 Prepare NSX for Cross-Region Support for VMware Cloud Foundation	14
Delete the NSX Controllers for VMware Cloud Foundation in Region B	15
Reconfigure the Network Interface on the NSX Edges for VMware Cloud Foundation in Region B	16
Power Off and Reconfigure the Virtual Machines of vRealize Log Insight in for VMware Cloud Foundation Region B	16
Delete the Universal Distributed Logical Router and Logical Switches for VMware Cloud Foundation in Region B	17
Assign the Secondary Role to NSX Manager for VMware Cloud Foundation in Region B	18
Reconfigure the Network Interface on the NSX Edges for VMware Cloud Foundation in Region B	20
Create an Application Virtual Network for vRealize Log Insight Virtual Machines for VMware Cloud Foundation in Region B	21
Add A Network Interface on the Universal Distributed Logical Router for VMware Cloud Foundation	22
Configure Dynamic Routing for VMware Cloud Foundation	23
Configure Universal Distributed Logical Router for Dynamic Routing for VMware Cloud Foundation in Region B	23
Verify Establishment of BGP for the Universal Distributed Logical Router for VMware Cloud Foundation in Region B	24
Configure Static Routes on the Universal Distributed Logical Router for VMware Cloud Foundation in Region B	26
4 Prepare vRealize Suite Products for Disaster Recovery	27
Reconfigure and Power on the Virtual Machines of vRealize Log Insight for VMware Cloud Foundation in Region B	27
Update the NTP Sources on vRealize Operations Manager for VMware Cloud Foundation in Region A	28
Place the Virtual Machines of a Management Solution in a Dedicated Folder for VMware Cloud Foundation	29
Move the Virtual Machines of vRealize Suite Lifecycle Manager, vRealize Automation, and vRealize Operations Manager to Dedicated Folders for VMware Cloud Foundation in Region A	29
Create Virtual Machine Folders for vRealize Automation and vRealize Operations Manager for VMware Cloud Foundation in Region B	30
Create the NSX Load Balancer for vRealize Automation and vRealize Operations Manager for VMware Cloud Foundation in Region B	31

Deploy the NSX Edge for Load Balancing vRealize Automation and vRealize Operations Manager for VMware Cloud Foundation in Region B 31

Disable the Interface on the vRealize NSX Edge Load Balancer for VMware Cloud Foundation in Region B 33

Configure the NSX Load Balancer for vRealize Automation and vRealize Operations Manager for VMware Cloud Foundation in Region B 34

Update Universal Logical Switch information on the SDDC manager for VMware Cloud Foundation in Region B 43

5 Deploy and Configure vSphere Replication for VMware Cloud Foundation 46

Prerequisites for the vSphere Replication Deployment for VMware Cloud Foundation in Region A 46

Deploy vSphere Replication for VMware Cloud Foundation in Region A 48

Deploy vSphere Replication for VMware Cloud Foundation in Region A 48

Replace the Certificate of vSphere Replication for VMware Cloud Foundation in Region A 50

Register vSphere Replication with vCenter Single Sign-On for VMware Cloud Foundation in Region A 51

Deploy vSphere Replication for VMware Cloud Foundation in Region B 52

Deploy the vSphere Replication Appliance for VMware Cloud Foundation in Region B 52

Replace the Certificate of vSphere Replication for VMware Cloud Foundation in Region B 54

Register vSphere Replication with vCenter Single Sign-On for VMware Cloud Foundation in Region B 55

Connect the vSphere Replication Instances for VMware Cloud Foundation 55

Isolate Network Traffic of vSphere Replication for VMware Cloud Foundation 56

Create a Port Group for vSphere Replication Traffic for VMware Cloud Foundation 57

Add a Network Adapter and Configure Static Routes for vSphere Replication for VMware Cloud Foundation 58

Create VMkernel Adapter for vSphere Replication on the ESXi Hosts for VMware Cloud Foundation 61

Configure Static Network Routes for VMware Cloud Foundation 62

6 Deploy and Configure Site Recovery Manager for VMware Cloud Foundation 64

Prerequisites for Installing Site Recovery Manager for VMware Cloud Foundation 65

Deploy Site Recovery Manager for VMware Cloud Foundation in Region A 66

Replace the Certificate of Site Recovery Manager for VMware Cloud Foundation in Region A 68

Configure the Site Recovery Manager Appliance for VMware Cloud Foundation in Region A 69

Deploy Site Recovery Manager for VMware Cloud Foundation in Region B 70

Replace the Certificate of Site Recovery Manager for VMware Cloud Foundation in Region B 71

Configure the Site Recovery Manager Appliance for VMware Cloud Foundation in Region B 72

Assign Licenses to the Site Recovery Manager Instances for VMware Cloud Foundation 73

Connect the Protected and Recovery Sites for VMware Cloud Foundation 74

Configure Mappings between the Protected and the Recovery Regions for VMware Cloud Foundation 75

7 Configure Operations Management for the Business Continuity Components for VMware Cloud Foundation 78

Connect vRealize Operations Manager to Site Recover Manager for VMware Cloud Foundation	78
Install the vRealize Operations Manager Management Pack for Site Recovery Manager for VMware Cloud Foundation	79
Add SRM Adapter Instances to vRealize Operations Manager for VMware Cloud Foundation	79
Connect vRealize Log Insight to Site Recovery Manager for VMware Cloud Foundation	80
Install the vRealize Log Insight Agent on Site Recovery Manager	81
Configure the vRealize Log Insight Agent on the Site Recovery Manager	82

8 Failover of the SDDC Management Applications for VMware Cloud Foundation 85

Complete the Configuration for Failover of the SDDC Management Applications for VMware Cloud Foundation	86
Configure Replication, Create Protection Group and Recovery Plan for the Operations Management Applications for VMware Cloud Foundation	87
Customize the Recovery Plan for the Operations Management Applications for VMware Cloud Foundation	89
Configure Replication, Create Protection Group and Recovery Plan for the Cloud Management Applications for VMware Cloud Foundation	90
Customize the Recovery Plan for the Cloud Management Platform for VMware Cloud Foundation	92
Create an Anti-Affinity Rule for vRealize Operations Manager for VMware Cloud Foundation in Region B	94
Create Anti-Affinity Rules for vRealize Automation for VMware Cloud Foundation in Region B	95
Create Virtual Machine Groups to Define the Startup Order of the Cloud Management Platform for VMware Cloud Foundation in Region B	96
Test Failover of the SDDC Management Applications for VMware Cloud Foundation	98
Test Failover of the Operations Management Applications for VMware Cloud Foundation	99
Test Failover of the Cloud Management Platform for VMware Cloud Foundation	100
Perform Planned Migration of the SDDC Management Applications for VMware Cloud Foundation	101
Initiate a Planned Migration of the Operations Management Applications for VMware Cloud Foundation	101
Initiate a Planned Migration of the Cloud Management Platform for VMware Cloud Foundation	103
Perform Disaster Recovery of the SDDC Management Applications for VMware Cloud Foundation	105
Assign the Primary Role to the NSX Manager Instance for the Management Cluster for VMware Cloud Foundation in Region B	106
Deploy the Control VM of the Universal Distributed Logical Router for VMware Cloud Foundation in Region B	107
Reconfigure the Universal Distributed Logical Router and NSX Edge Nodes for Dynamic Routing for VMware Cloud Foundation in Region B	108
Verify Establishment of BGP for the Universal Distributed Logical Router for VMware Cloud Foundation in Region B	111
Deploy the NSX Controllers for the NSX Instance for VMware Cloud Foundation in Region B	111
Connect the Application NSX Load Balancer in Region B to the SDDC Network for VMware Cloud Foundation	113
Initiate Disaster Recovery of the Operations Management Applications for VMware Cloud Foundation in Region B	114

Initiate Disaster Recovery of the Cloud Management Platform for VMware Cloud Foundation in Region B 115

Post-Failover Configuration of the SDDC Management Applications for VMware Cloud Foundation 116

Additional Post-Failover Configuration After Region A Is Available Again for VMware Cloud Foundation 119

9 Failback of the SDDC Management Applications for VMware Cloud Foundation 127

Test Failback of the SDDC Management Applications for VMware Cloud Foundation 128

Test Failback of the Operations Management Applications for VMware Cloud Foundation 128

Test Failback of the Cloud Management Platform for VMware Cloud Foundation 129

Perform Failback as Planned Migration of the SDDC Management Applications for VMware Cloud Foundation 131

Initiate Failback as a Planned Migration of the Operations Management Applications for VMware Cloud Foundation 131

Initiate Failback as a Planned Migration of the Cloud Management Platform for VMware Cloud Foundation 133

Perform Failback as Disaster Recovery of the SDDC Management Applications for VMware Cloud Foundation 135

Assign the Primary Role to the NSX Manager Instance for the Management Cluster for VMware Cloud Foundation in Region A 136

Redeploy the Control VM of the Universal Distributed Logical Router for VMware Cloud Foundation in Region A 137

Reconfigure the Universal Distributed Logical Router and NSX Edge Nodes for Dynamic Routing for VMware Cloud Foundation in Region A 139

Verify the Establishment of BGP for the Universal Distributed Logical Router for VMware Cloud Foundation in Region A 141

Deploy the NSX Controllers for the NSX Instance for VMware Cloud Foundation in Region A 141

Connect the Application NSX Load Balancer for VMware Cloud Foundation in Region A to the SDDC Network 143

Update the vSAN Default Storage Policy of the Management Cluster for VMware Cloud Foundation in Region A 144

Initiate Disaster Recovery of the Operations Management Applications for VMware Cloud Foundation in Region A 144

Initiate Disaster Recovery of the Cloud Management Platform for VMware Cloud Foundation in Region A 146

Post-Failback Configuration of the SDDC Management Applications for VMware Cloud Foundation 147

Additional Post-Failback Configuration After Region B Is Available Again for VMware Cloud Foundation 149

10 Reprotect of the SDDC Management Applications for VMware Cloud Foundation 155

Prerequisites for Performing Reprotect for VMware Cloud Foundation 155

Reprotect the Operations Management Applications for VMware Cloud Foundation 156

Reprotect the Cloud Management Platform for VMware Cloud Foundation 158

About VMware Cloud Foundation 3.9.1 Site Protection and Recovery

Site Protection and Recovery for VMware Cloud Foundation provides step-by-step instructions for adapting a dual-region software-defined data center (SDDC), deployed on top of VMware Cloud Foundation, to provide disaster recovery of the SDDC management components.

Use VMware Site Recovery Manager™ and VMware vSphere® Replication™ to perform site protection and recovery of VMware vRealize® Automation™ with embedded VMware vRealize® Orchestrator™, VMware vRealize® Operations Manager™ analytics cluster, and VMware vRealize® Suite Lifecycle Manager™.

Deployment and configuration of vRealize Automation, vRealize Suite Lifecycle Manager, and vRealize Operations Manager are out of scope for this document and must be configured separately. The *Site Protection and Recovery for VMware Cloud Foundation* documentation covers both failover to the recovery region and failback to the protected region.

Table 1-1. Support for Failover/Failback of the SDDC Management Applications

Management Component	Supports Failover
vRealize Suite Lifecycle Manager	Yes
vRealize Operations Manager analytics nodes	Yes
vSphere proxy agents	No
vRealize Automation appliance	Yes
Microsoft SQL server	Yes
vRealize Automation IaaS Components	Yes

Intended Audience

The *Site Protection and Recovery for VMware Cloud Foundation* documentation is intended for cloud architects, infrastructure administrators, cloud administrators and cloud operators who are familiar with and want to use VMware software to deploy in a short time and manage an SDDC that meets the requirements for capacity, scalability, backup and restore, and disaster recovery.

Required VMware Software

The documentation is compliant and validated the following VMware software. *Site Protection and Recovery for VMware Cloud Foundation*

Product	Version
VMware Cloud Foundation	3.9.1
VMware Site Recovery Manager	8.2
VMware vSphere Replication	8.2

Failover and Failback Checklist for the SDDC Management Applications for VMware Cloud Foundation



Use a checklist to verify that you have fulfilled all the requirements to initiate disaster recovery or planned migration of the SDDC management applications and to complete the configuration of these applications.

Table 1-1. Checklist for Failover and Failback in an SDDC

Checklist	Tasks
Activation and Assessment	<ul style="list-style-type: none">■ Verify that the disaster failover or failback is required:<ul style="list-style-type: none">■ For example, an application failure might not be a cause for a failover or failback, while an extended region outage is a valid cause.■ Plan for business continuity events such as scheduled building maintenance or the probability of a natural disaster.
Approval	<ul style="list-style-type: none">■ Submit the required documentation for approval to the following roles:<ul style="list-style-type: none">■ IT management staff■ CTO■ Business users■ Other stakeholders
Activation Logistics	<ul style="list-style-type: none">■ Verify that all the required facilities and personnel are available for the complete duration of the disaster recovery process.■ Verify that Site Recovery Manager is available in the recovery region.■ Verify the replication status of the applications.■ Verify the state of the NSX Edge nodes in the recovery region:<ul style="list-style-type: none">■ Verify that the NSX Edge nodes are available.■ Verify that the IP addresses for the VXLAN backed networks are correct.■ Verify that the application load balancer on the NSX Edge node is correctly configured according to the design.■ Verify that the firewall on the NSX Edge node is correctly configured according to the design.

Table 1-1. Checklist for Failover and Failback in an SDDC (continued)

Checklist	Tasks
Communication, Initiation, and Failover or Failback Validation	<ul style="list-style-type: none"> ■ In case of a planned migration: <ul style="list-style-type: none"> ■ Notify all stakeholders for the planned outage and the expected duration of the maintenance window. ■ At the scheduled time, initiate the failover or failback process. ■ In case of a failover or failback for disaster recovery: <ul style="list-style-type: none"> ■ Before initiating a failover or a failback, notify all stakeholders for the event. ■ After completing a failover or a failback: <ul style="list-style-type: none"> ■ Test applications availability. ■ Notify all stakeholders for the completed event.
Multiple Availability Zones	<p>If your environment consists of multiple availability zones, perform additional configuration for failback for disaster recovery:</p> <ul style="list-style-type: none"> ■ In case of failback for disaster recovery in which Region B remains unavailable, the vSAN witness appliance is not available too. As a result, you might be unable to provision the vRealize Suite virtual machines in Region A according to the active vSAN storage policy. To enable the recovery of the vRealize Suite virtual machines, turn on the force-provisioning option in the storage policy. ■ In case of a planned migration in which Region A and Region B are still operational, the vSAN witness appliance is available and the active storage policy is satisfied.
Configuration After Failover or Failback	<p>In case of disaster recovery failover or failback, perform additional configuration:</p> <ul style="list-style-type: none"> ■ Configure the NSX Controllers and the UDLR control VM to forward events to vRealize Log Insight in the recovery region. ■ Redirect the log data from the failed over or failed back applications to vRealize Log Insight in the recovery region. ■ Complete a post-recovery assessment: <ul style="list-style-type: none"> ■ Note which items worked and which did not work, and identify improvements that you can include in the recovery plan.

Prerequisites for Implementing Disaster Recovery on VMware Cloud Foundation

2

Before you implement disaster recovery in VMware Cloud Foundation, your environment must support certain prerequisites for deployment and networking.

You implement disaster recovery for vRealize Automation, vRealize Suite Lifecycle Manager, and vRealize Operations Manager. The disaster recovery scenario of the Cloud Management and the Operations Management platforms are validated and require the following prerequisites.

Disaster Recovery Considerations

When you prepare for disaster recovery, you must determine which of your two Cloud Foundation instances will function as the protected site and which one as the recovery site.

The protected site hosts the business-critical SDDC services. In the context of Cloud Foundation, the protected site contains the vRealize products, including vRealize Operations Manager, vRealize Suite Lifecycle Manager and vRealize Automation, with failover that is enabled in the event of a disaster.

The recovery site is an alternative location to which these vRealize applications are migrated and hosted in the event of a disaster.

In this guide, the protected site is referred to as Region A and the recovery site is referred to as Region B.

Disaster Recovery Prerequisites

Before you implement disaster recovery, verify that your environment satisfies the following prerequisites:

- Download the VMware Site Recovery Manager 8.2 .iso image and mount it on the machine that you use to access the vSphere Client. In each region, provide the environment configuration for Site Recovery Manager deployment.

Attribute	Protected site	Recovery Site
Cluster	sfo01-m01-mgmt01	lax01-m01-mgmt01
Datastore	sfo01-m01-vsan01	lax01-m01-vsan01
Number of CPUs	2	2
Memory (GB)	8	8

Attribute	Protected site	Recovery Site
Disk space (GB)	20	20
Virtual machine network	sfo01-m01-vds01-management	lax01-m01-vds01-management

- Download the vSphere Replication 8.2 .iso image and mount it on the machine that you use to access the vSphere Web Client. In each region, provide the environment configuration for deploying the vSphere Replication virtual appliance.

Attribute	Protected site	Recovery Site
Cluster	sfo01-m01-mgmt01	lax01-m01-mgmt01
Datastore	sfo01-m01-vsan01	lax01-m01-vsan01
Number of CPUs	4	4
Memory (GB)	8	8
Disk space (GB)	26	26
Virtual machine network	sfo01-m01-vds01-management	lax01-m01-vds01-management

- Obtain a license for Site Recovery Manager.

Cloud Foundation Prerequisites

- Verify that VMware Cloud Foundation is version 3.9.1.
- Verify that you have obtained a Cloud Foundation license that covers the use of cross-vCenter NSX objects.
- Deploy vRealize Suite Lifecycle Manager, vRealize Automation, and vRealize Operations Manager in Region A after you deploy or upgrade VMware Cloud Foundation to 3.9.1.
- Temporarily migrate all virtual machines on NSX logical switches to VLAN-backed distributed port groups to keep their connectivity and disconnect the virtual machines from the logical switches. You can reconnect these virtual machines to the logical switches after NSX is configured for cross vCenter Server operations.

Networking Prerequisites

- The regions must be connected to each other and the connection must support jumbo frames and Layer 3 routing between the regions.
- All uplinks, port channels, and VLANs that carry VXLAN and vSphere Replication traffic must be configured for jumbo frames.
- The maximum supported latency between regions must be 150 ms.
- Sufficient bandwidth must be available for replication traffic. See vSphere Replication Calculator at <http://www.vmware.com/vrcalculator> for the initial guidance.
- BGP must be licensed and available for use on the Layer 3 devices in both regions.

- If you upgrade Cloud Foundation to 3.9.1 and do not have application virtual networks configured, contact VMware Support for additional guidance on configuration and migration of application virtual networks, before performing disaster recovery or planned migration.
- Nexus switches must be updated to a Nexus OS release that supports routing protocol adjacencies over virtual port channels. See <https://www.cisco.com/c/en/us/support/docs/ip/ip-routing/118997-technote-nexus-00.html> for the minimum required Nexus OS release and additional configuration required.

Prepare NSX for Cross-Region Support for VMware Cloud Foundation

3

The first step in configuring disaster recovery is to configure cross-region NSX to enable workload mobility.

Configure NSX for cross-region support of universal objects. Due to the default configuration of NSX within VMware Cloud Foundation, NSX must be reconfigured to support universal objects. If you select to use default networks during VMware Cloud Foundation bring-up, you must remove NSX objects that were deployed and you must update the hosts VTEPs to use unique routable IP addresses.

Note NSX cross-site on the management domain is not supported within a rack.

Procedure

1 [Delete the NSX Controllers for VMware Cloud Foundation in Region B](#)

For a dual-region setup, cross-vCenter NSX controllers are also deployed in Region B which contains the primary NSX Manager. You must remove the NSX controller cluster in the recovery region.

2 [Reconfigure the Network Interface on the NSX Edges for VMware Cloud Foundation in Region B](#)

Before deleting the configured logical switches, disconnect them from the ESG nodes and assign them to a VLAN-backed port group until a secondary NSX manager role is assigned.

3 [Power Off and Reconfigure the Virtual Machines of vRealize Log Insight in for VMware Cloud Foundation Region B](#)

Before deleting the configured logical switches, disconnect them from the Virtual Machines of vRealize Log Insight in Region B. Assign to a VLAN-backed port group until secondary NSX manager role is assigned. The virtual machines must be powered off before migration as IP connectivity to or from the application virtual network is not available at this stage.

4 [Delete the Universal Distributed Logical Router and Logical Switches for VMware Cloud Foundation in Region B](#)

For a dual-region setup, Universal Distributed Logical Router(UDLR) and Logical Switches are deployed in the recovery region. You must remove them before assigning secondary role to NSX manager role in region B.

5 Assign the Secondary Role to NSX Manager for VMware Cloud Foundation in Region B

To enable cross-vCenter NSX networking, configure the NSX Manager in Region B as a secondary. You perform this operation from the primary NSX Manager which is in Region A. You join the management cluster in Region B to the universal transport zone from the local vCenter Server.

6 Reconfigure the Network Interface on the NSX Edges for VMware Cloud Foundation in Region B

After secondary role is assigned to the NSX Manager in region B, universal logical switches are available in the region B. Reconfigure the Network Interface on the NSX Edges in Region B to use those Logical Switches.

7 Create an Application Virtual Network for vRealize Log Insight Virtual Machines for VMware Cloud Foundation in Region B

Create an Application Virtual Network for vRealize Log Insight Virtual Machines in Region B.

8 Add A Network Interface on the Universal Distributed Logical Router for VMware Cloud Foundation

Add a Network Interface on the Universal Distributed Logical Router for vRealize Log Insight virtual machines in region B

9 Configure Dynamic Routing for VMware Cloud Foundation

Dynamic routing enables the dynamic discovery of the IP subnets configured on NSX virtual wires by the physical network and vice versa.

Delete the NSX Controllers for VMware Cloud Foundation in Region B

For a dual-region setup, cross-vCenter NSX controllers are also deployed in Region B which contains the primary NSX Manager. You must remove the NSX controller cluster in the recovery region.

Procedure

- 1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Settings	Value
URL	https://lax01m01vc01.lax01.rainpole.local/ui
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Networking and security** inventory, click **Installation and upgrade**.
- 3 On the **Management** tab, click the **NSX Controller nodes** tab, and, from the **NSX Manager** drop-down menu, select **172.17.11.65**.
- 4 Select the first NSX Controller node and click the **Delete** button.
On the **Delete Controller** dialog box, click **Delete**.
- 5 Repeat this step to delete the remaining two controllers.

Reconfigure the Network Interface on the NSX Edges for VMware Cloud Foundation in Region B

Before deleting the configured logical switches, disconnect them from the ESG nodes and assign them to a VLAN-backed port group until a secondary NSX manager role is assigned.

You temporarily migrate the ESG nodes on NSX logical switches to VLAN-backed distributed port groups to keep their connectivity and disconnect the virtual machines from the logical switches. You can reconnect these virtual machines to the logical switches after NSX is configured for cross vCenter Server operations.

Procedure

- 1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Settings	Value
URL	https://lax01m01vc01.lax01.rainpole.local/ui
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Networking and security** inventory, click **NSX Edges**.
- 3 From the **NSX Manager** drop-down menu, select **172.17.11.65**.
- 4 Click the **lax01m01esg01** node and on the **NSX Edges** page, click the **Configure** tab.
- 5 Click **Interfaces**, select the **lax01m01udlr01** interface, to which the Universal Transit Network is connected, and click **Edit**.
- 6 On the **Edit interface** dialog box, configure the settings and click **Save**.

Setting	ESG Node 1 - lax01m01esg01
Name	lax01m01udlr01
Connected to	lax01-m01-vds01-management
Connectivity status	Disconnected

- 7 Repeat the step on the lax01m01esg02 ESG Node.

Power Off and Reconfigure the Virtual Machines of vRealize Log Insight in for VMware Cloud Foundation Region B

Before deleting the configured logical switches, disconnect them from the Virtual Machines of vRealize Log Insight in Region B. Assign to a VLAN-backed port group until secondary NSX manager role is assigned. The virtual machines must be powered off before migration as IP connectivity to or from the application virtual network is not available at this stage.

Procedure

- 1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Settings	Value
URL	https://lax01m01vc01.lax01.rainpole.local/ui
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **VMs and templates** inventory, expand the **lax01m01vc01.lax01.rainpole.local** tree and expand the **lax01-m01dc** data center.
- 3 Select the **Management VMs** folder and click the **VMs** tab.
- 4 Power off the vRealize Log Insight virtual machines in the following order.

Virtual Machine Name	Description	Shutdown Order
lax01vrli01c	vRealize Log Insight worker node	1
lax01vrli01b	vRealize Log Insight worker node	2
lax01vrli01a	vRealize Log Insight master node	3

- 5 Migrate vRealize Log Insight virtual machines to a VLAN-backed port group.
 - a Right-click vRealize Log Insight master node **lax01vrli01a** and select **Edit settings**.
 - b On the **Edit settings** dialog box, click the **Virtual hardware** tab.
 - c From the **Network adapter 1** drop-down menu, click **Browse**, select the VLAN-backed distributed port group **lax01-m01-vds01-management**, and click **OK**.
 - d Repeat these steps for the lax01vrli01b and lax01vrli01c vRealize Log Insight worker nodes.

Delete the Universal Distributed Logical Router and Logical Switches for VMware Cloud Foundation in Region B

For a dual-region setup, Universal Distributed Logical Router(UDLR) and Logical Switches are deployed in the recovery region. You must remove them before assigning secondary role to NSX manager role in region B.

Procedure

- 1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Settings	Value
URL	https://lax01m01vc01.lax01.rainpole.local/ui
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Networking and security** inventory, click **NSX Edges**.
- 3 Delete the Universal Distributed Logical Router for Region B.
 - a In the **Networking and security** inventory, click **NSX Edges**.
 - b From the **NSX Manager** drop-down menu, select **172.17.11.65**.
 - c Select the Universal Distributed Logical Router **lax01m01udlr01** and click **Delete**.
On the **Delete NSX Edge** dialog box, click **Delete**.
- 4 Delete the Logical Switches for Region B.
 - a In the **Networking and security** inventory, click **Logical switches**.
 - b From the **NSX Manager** drop-down menu, select **172.17.11.65**.
 - c Select the **Universal Transit Network** logical switch and click **Delete**.
On the **Delete Logical Switches** dialog box, click **Delete**.
 - d Repeat this step to delete the Mgmt-RegionA01-VXLAN and Mgmt-xRegion01-VXLAN logical switches.

Assign the Secondary Role to NSX Manager for VMware Cloud Foundation in Region B

To enable cross-vCenter NSX networking, configure the NSX Manager in Region B as a secondary. You perform this operation from the primary NSX Manager which is in Region A. You join the management cluster in Region B to the universal transport zone from the local vCenter Server.

Procedure

- 1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Settings	Value
URL	https://lax01m01vc01.lax01.rainpole.local/ui
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Change the Segment ID allocation.
 - a In the **Networking and security** inventory, click **Installation and upgrade**, and click the **Logical network settings** tab.
 - b From the **NSX Manager** drop-down menu, select **172.17.11.65**.

- c In the **Segment IDs** section, click **Edit**.
- d In the **Edit Segment ID Settings** dialog box, remove **Universal Segment ID pool** values, deselect **Universal Multicast addressing**, enter the following settings, and click **Save**.

Setting	Value
Segment ID pool	6000-6200
Multicast addressing	On
Multicast addresses	239.5.0.0-239.5.255.255
Universal Segment ID pool	-
Universal Multicast addressing	Off
Universal Multicast addresses	-

Important Ensure that the Segment ID pool does not overlap with the Segment ID pool of the NSX Manager in Region A.

3 Remove the primary role from the Management NSX Manager in Region B

- a On the **Installation and upgrade** page, click the **Management** tab.
- b Select the **lax01m01nsx01** NSX Manager for Region B and, from the **Actions** drop-down menu, select **Remove primary role**.

On the **Remove primary role** confirmation dialog box, click **Yes**. The operation sets the role of the NSX Manager instance to Transit.

4 Assign the secondary role to the Management NSX Manager in Region B.

- a On the **Installation and upgrade** page, click the **Management** tab.
- b Select the **sfo01m01nsx01** NSX Manager for Region A and, from the **Actions** drop-down menu, select **Add secondary manager**.
- c In the **New secondary manager** dialog box, configure the settings and click **Add**.

Setting	Value
Primary NSX Manager	sfo01m01nsx01
NSX Manager	lax01m01nsx01
User name	admin
Password	<i>mgmtnsx_admin_password</i>
Confirm password	<i>mgmtnsx_admin_password</i>

- d In the **Thumbprint confirmation** dialog box, click **Accept**.

The operation sets the role of the management NSX Manager in Region B to Secondary.

- 5 Verify that Universal Logical Switches are visible in Region B.
 - a On the **Installation and upgrade** page, click the **Logical switches** tab.
 - b From the **NSX Manager** drop-down menu, select the **172.17.11.65** NSX Manager instance for Region B.
 - c Verify that Universal Logical Switches are visible in the **Logical switches** page.

Reconfigure the Network Interface on the NSX Edges for VMware Cloud Foundation in Region B

After secondary role is assigned to the NSX Manager in region B, universal logical switches are available in the region B. Reconfigure the Network Interface on the NSX Edges in Region B to use those Logical Switches.

You perform this procedure for the NSX Edges in Region B.

Setting	Value for lax01m01esg01	Value for lax01m01esg02
Name	lax01m01udlr01	lax01m01udlr01
Connected to	Universal Transit Network	Universal Transit Network
Connectivity status	Connected	Connected

Procedure

- 1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Settings	Value
URL	https://lax01m01vc01.lax01.rainpole.local/ui
User name	administrator@vsphere.local
Password	<i>vsphere_admin_password</i>

- 2 In the **Networking and security** inventory, click **NSX Edges**.
- 3 From the **NSX Manager** drop-down menu, select **172.17.11.65**.
- 4 Click the **lax01m01esg01** node and on the **NSX Edges** page, click the **Configure** tab.
- 5 Click **Interfaces**, select the **lax01m01udlr01** interface, and click **Edit**.
- 6 On the **Edit interface** dialog box, configure the settings and click **Save**.

Setting	ESG Node 1 - lax01m01esg01
Name	lax01m01udlr01
Connected to	Universal Transit Network
Connectivity status	Connected

7 Configure static routes.

- a On the **NSX Edges** page, click the **Routing** tab.
- b Click the **Static routes** tab, and click **Add**.
- c On the New static route dialog box, configure the settings and click **Add**.

Setting	Value
Network	192.168.31.0/24
Interface	lax01m01udlr01
Admin distance	210

- d On the **Static route** page, click **Publish**.

8 Configure BGP routing.

- a Click the **BGP** tab.
- b In the **Neighbors** section, select the IP address of **lax01m01udlr01** and click **Edit**.
- c In the **Edit BGP configuration** dialog box, configure the settings and click **Save**.

Setting	Value
IP Address	192.168.10.4
Remote AS	65003
Weight	10
Keep Alive Time	1
Hold Down Time	3
Password	<i>BGP_password</i>

- d On the **BGP** page, click **Publish**.

9 Repeat this procedure for the lax01m01esg02 ESG Node.

Create an Application Virtual Network for vRealize Log Insight Virtual Machines for VMware Cloud Foundation in Region B

Create an Application Virtual Network for vRealize Log Insight Virtual Machines in Region B.

Procedure

- 1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Settings	Value
URL	https://lax01m01vc01.lax01.rainpole.local/ui
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Networking and security** inventory, click **Logical switches**.
- 3 From the **NSX Manager** drop-down menu, select **172.16.11.65**.
- 4 On the **Logical switches** page, click **Add**.
- 5 In the **New Logical Switch** dialog box, configure the settings and click **Add**.

Setting	Value
Name	Mgmt-RegionB01-VXLAN
Transport Zone	Mgmt Universal Transport Zone
Replication Mode	Hybrid

Add A Network Interface on the Universal Distributed Logical Router for VMware Cloud Foundation

Add a Network Interface on the Universal Distributed Logical Router for vRealize Log Insight virtual machines in region B

Procedure

- 1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Settings	Value
URL	https://lax01m01vc01.lax01.rainpole.local/ui
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Networking and security** inventory, click **NSX Edges**.
- 3 From the **NSX Manager** drop-down menu, select **172.16.11.65**.
- 4 Click the edge link of **sfo01m01udlr01** Universal Distributed Logical Router and click the **Configure** tab.
- 5 Click **Interfaces** and click **Add**.

6 On the **New interface** dialog box, configure the settings and click **Add**.

Setting	Value
Interface name	Mgmt-RegionB01-VXLAN
Type	Internal
Connected to	Mgmt-RegionB01-VXLAN
Connectivity status	Connected
Primary IP Address	192.168.32.1
Subnet Prefix Length	24

Configure Dynamic Routing for VMware Cloud Foundation

Dynamic routing enables the dynamic discovery of the IP subnets configured on NSX virtual wires by the physical network and vice versa.

Configure Universal Distributed Logical Router for Dynamic Routing for VMware Cloud Foundation in Region B

Configure the universal distributed logical router (UDLR) to use dynamic routing in Region B.

Procedure

1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Settings	Value
URL	https://lax01m01vc01.lax01.rainpole.local/ui
User name	administrator@vsphere.local
Password	<i>vsphere_admin_password</i>

- 2 In the **Networking and security** inventory, click **NSX Edges**.
- 3 From the **NSX Manager** drop-down menu, select **172.16.11.65**.
- 4 Configure the Universal Distributed Logical Router.
 - a Click **sfo01m01udlr01** and click the **Routing** tab.
 - b In the left pane, click **BGP**, and, in the **Neighbors** section, click **Add**.

- c In the **Add BGP neighbor** dialog box, configure the settings for both NSX Edge devices, and click **OK**.

Setting	Value for lax01m01esg01	Value for lax01m01esg02
IP address	192.168.10.50	192.168.10.51
Forwarding address	192.168.10.3	192.168.10.3
Protocol address	192.168.10.4	192.168.10.4
Remote AS	65003	65003
Weight	10	10
Keep alive time	1	1
Hold down time	3	3
Password	<i>BGP_password</i>	<i>BGP_password</i>

- d On the **NSX Edges** page, click **Publish**.

Verify Establishment of BGP for the Universal Distributed Logical Router for VMware Cloud Foundation in Region B

Verify that the UDLR is successfully peering and BGP routing has been established.

Procedure

- 1 Log in to the Universal Distributed Logical Router by using a Secure Shell (SSH) client.

Setting	Value
Hostname	sfo01m01udlr01
User name	admin
Password	<i>udlr_admin_password</i>

- 2 Run the `show ip bgp neighbors` command to display information about the BGP and TCP connections to neighbors.

The BGP State shows `Established`, `UP` if you have successfully peered with the Edge Service Gateway.

```

192.168.10.4 - PuTTY
BGP neighbor is 192.168.10.1, remote AS 65003,
BGP state = Established, up
Hold time is 3, Keep alive interval is 1 seconds
Neighbor capabilities:
  Route refresh: advertised and received
  Address family IPv4 Unicast:advertised and received
  Graceful restart Capability:advertised and received
  Restart remain time: 0
Received 351566 messages, Sent 351576 messages
Default minimum time between advertisement runs is 30 seconds
For Address family IPv4 Unicast:advertised and received
  Index 1 Identifier 0x3b7a3cc
  Route refresh request:received 0 sent 0
  Prefixes received 8 sent 3 advertised 3
Connections established 2, dropped 1
Local host: 192.168.10.4, Local port: 179
Remote host: 192.168.10.1, Remote port: 21217

BGP neighbor is 192.168.10.2, remote AS 65003,
BGP state = Established, up
Hold time is 3, Keep alive interval is 1 seconds
Neighbor capabilities:
  Route refresh: advertised and received
  Address family IPv4 Unicast:advertised and received
  Graceful restart Capability:advertised and received
  Restart remain time: 0
Received 351547 messages, Sent 351560 messages
byte 1108
    
```

- 3 Run the `show ip route` command to verify that you are receiving routes using BGP, and that there are multiple routes to BGP learned networks.

The letter B before the route indicates that BGP is used.

```

192.168.10.4 - PuTTY
UDLR01-0> show ip route

Codes: O - OSPF derived, I - IS-IS derived, B - BGP derived,
C - connected, S - static, L1 - IS-IS level-1, L2 - IS-IS level-2,
IA - OSPF inter area, E1 - OSPF external type 1, E2 - OSPF external type 2,
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

Total number of routes: 16

B    0.0.0.0/0          [200/0]    via 192.168.10.1
B    0.0.0.0/0          [200/0]    via 192.168.10.2
B    10.159.4.0/23      [200/0]    via 192.168.10.1
B    10.159.4.0/23      [200/0]    via 192.168.10.2
C    169.254.1.0/30     [0/0]      via 169.254.1.1
B    172.16.11.0/24     [200/0]    via 192.168.10.1
B    172.16.11.0/24     [200/0]    via 192.168.10.2
B    172.16.21.0/24     [200/0]    via 192.168.10.1
B    172.16.21.0/24     [200/0]    via 192.168.10.2
B    172.17.11.0/24     [200/0]    via 192.168.10.1
B    172.17.11.0/24     [200/0]    via 192.168.10.2
B    172.17.21.0/24     [200/0]    via 192.168.10.1
B    172.17.21.0/24     [200/0]    via 192.168.10.2
B    172.27.11.0/24     [200/0]    via 192.168.10.1
B    172.27.11.0/24     [200/0]    via 192.168.10.2
B    172.27.12.0/24     [200/0]    via 192.168.10.1
B    172.27.12.0/24     [200/0]    via 192.168.10.2
B    172.27.14.0/24     [200/0]    via 192.168.10.1
B    172.27.14.0/24     [200/0]    via 192.168.10.2
B    172.27.15.0/24     [200/0]    via 192.168.10.1
B    172.27.15.0/24     [200/0]    via 192.168.10.2
B    172.27.22.0/24     [200/0]    via 192.168.10.1
B    172.27.22.0/24     [200/0]    via 192.168.10.2
C    192.168.10.0/24     [0/0]      via 192.168.10.4
C    192.168.11.0/24     [0/0]      via 192.168.11.1
C    192.168.31.0/24     [0/0]      via 192.168.31.1
C    192.168.32.0/24     [0/0]      via 192.168.32.1
UDLR01-0>
    
```

Configure Static Routes on the Universal Distributed Logical Router for VMware Cloud Foundation in Region B

Configure the universal distributed logical router (UDLR) to use static routes for routing to the management servers in Region B.

Procedure

- 1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Settings	Value
URL	https://lax01m01vc01.lax01.rainpole.local/ui
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Configure the Universal Distributed Logical Router static routes.

- a In the **Networking and security** inventory, click **NSX Edges**.
- b From the **NSX Manager** drop-down menu, select **172.16.11.65**.
- c Click **sfo01m01udlr01** and click the **Routing** tab.
- d In the left pane, click **Static routes** and click **Add**.
- e In the **New static route** dialog box, configure the settings and click **OK**.

Setting	Value
Network	172.17.11.0/24
Next hop	192.168.10.50,192.168.10.51
Admin distance	1

- f Click **Publish**.

Prepare vRealize Suite Products for Disaster Recovery

4

This chapter includes the following topics:

- [Reconfigure and Power on the Virtual Machines of vRealize Log Insight for VMware Cloud Foundation in Region B](#)
- [Update the NTP Sources on vRealize Operations Manager for VMware Cloud Foundation in Region A](#)
- [Place the Virtual Machines of a Management Solution in a Dedicated Folder for VMware Cloud Foundation](#)
- [Create the NSX Load Balancer for vRealize Automation and vRealize Operations Manager for VMware Cloud Foundation in Region B](#)
- [Update Universal Logical Switch information on the SDDC manager for VMware Cloud Foundation in Region B](#)

Reconfigure and Power on the Virtual Machines of vRealize Log Insight for VMware Cloud Foundation in Region B

After adding application virtual network for vRealize Log Insight virtual machines in region B and configuring dynamic routing, connect the virtual machines of vRealize Log Insight in Region B to the application virtual network. Power on the vRealize Log Insight as per the start up order.

Procedure

- 1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Settings	Value
URL	<code>https://lax01m01vc01.lax01.rainpole.local/ui</code>
User name	<code>administrator@vsphere.local</code>
Password	<code>vsphere_admin_password</code>

- 2 In the **VMs and templates** inventory, expand the **lax01m01vc01.lax01.rainpole.local** tree and expand the **lax01-m01dc** data center.
- 3 Select the **Management VMs** folder and click the **VMs** tab.

- 4 Migrate vRealize Log Insight virtual machines to **Mgmt-RegionB01-VXLAN** logical switch.
 - a Right-click the **lax01vrli01a** vRealize Log Insight master node and select **Edit settings**.
 - b On the **Edit Settings** dialog box, click the **Virtual hardware** tab.
 - c Under **Network adapter 1**, from the drop-down menu, select **Browse**, select the **Mgmt-RegionB01-VXLAN** logical switch, and click **OK**.
 - d Repeat this step for the lax01vrli01b and lax01vrli01c vRealize Log Insight worker nodes.
- 5 Power on the vRealize Log Insight virtual machines in the following order.

Virtual Machine Name	Description	Startup Order
lax01vrli01a	vRealize Log Insight master node	1
lax01vrli01b	vRealize Log Insight worker node	2
lax01vrli01c	vRealize Log Insight worker node	3

Update the NTP Sources on vRealize Operations Manager for VMware Cloud Foundation in Region A

Before you fail over vRealize Operations Manager between regions, update the NTP synchronization settings with an NTP server in each region.

Procedure

- 1 Log in to the master node of vRealize Operations Manager by using a Secure Shell (SSH) client.

Setting	Value
FQDN	vrops01svr01a.rainpole.local
User name	root
Password	<i>vrops_root_password</i>

- 2 Open the `/etc/ntp.conf` file in edit mode.

```
vi /etc/ntp.conf
```

- 3 Locate the `## CaSA Section Start #` section of the file.
- 4 Add the two NTP servers for Region A and Region B.

```
server ntp.sfo01.rainpole.local iburst prefer
server ntp.lax01.rainpole.local iburst prefer
```

- 5 Save the file.

```
!wq
```

- 6 Restart the NTP service.

```
service ntp restart
```

- 7 Repeat the procedure for the vrops01svr01b.rainpole.local master replica and the vrops01svr01c.rainpole.local data node.

Place the Virtual Machines of a Management Solution in a Dedicated Folder for VMware Cloud Foundation

Virtual machine folders provide a logical grouping of virtual machines. You place the virtual machines of vRealize Automation and of vRealize Operations Manager in to dedicated folders. You later create a mapping between these folders in Site Recovery Manager as a part of the fail-over setup.

Move the Virtual Machines of vRealize Suite Lifecycle Manager, vRealize Automation, and vRealize Operations Manager to Dedicated Folders for VMware Cloud Foundation in Region A

Create folders to group the virtual machines of vRealize Automation and vRealize Operations Manager, and move the virtual machines there. You use the folders for easier configuration of virtual machine replication.

Procedure

- 1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Setting	Value
URL	https://sfo01m01vc01.sfo01.rainpole.local/ui
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Create folders for vRealize Automation and vRealize Operations Manager virtual machines.
 - a In the **VMs and templates** inventory, expand the **sfo01m01vc01.sfo01.rainpole.local** tree and expand the **sfo01-m01dc** data center.
 - b Right-click **sfo01-m01dc** and select **New folder > New VM and template folder**.
 - c In the **New folder** dialog box, enter **sfo01-m01fd-vra** and click **OK**.
 - d Repeat step to create the **sfo01-m01fd-vrops** folder.

3 In the **VMs** tab, move the virtual machines to the respective destination folders.

Component	Virtual Machine	Destination Folder
vRealize Suite Lifecycle Manager	vrslcm01svr01	Management VMs
vRealize Automation	<ul style="list-style-type: none"> ■ vra01svr01a ■ vra01svr01b ■ vra01svr01c ■ vra01iws01 ■ vra01iws01a ■ vra01iws01b ■ vra01ims01 ■ vra01dem01a ■ vra01dem01b ■ vra01mssql01 	sfo01-m01fd-vra
vRealize Operations Manager	<ul style="list-style-type: none"> ■ vrops01svr01 ■ vrops01svr01b ■ vrops01svr01c 	sfo01-m01fd-vrops

Create Virtual Machine Folders for vRealize Automation and vRealize Operations Manager for VMware Cloud Foundation in Region B

Create folders to group the virtual machines of vRealize Automation and vRealize Operations Manager in Region B. You use the folders in folder mapping when a failover between the regions occurs.

Procedure

1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Settings	Value
URL	https://lax01m01vc01.lax01.rainpole.local/ui
User name	administrator@vsphere.local
Password	vsphere_admin_password

2 Create folders for vRealize Automation and vRealize Operations Manager virtual machines.

- a In the **VMs and templates** inventory, expand the **lax01m01vc01.lax01.rainpole.local** tree and expand the **lax01-m01dc** data center.
- b Right-click **lax01-m01dc** and select **New folder > New VM and template folder**.
- c In the **New folder** dialog box, enter **lax01-m01fd-vra** and click **OK**.
- d Repeat step to create the **lax01-m01fd-vrops** folder.

Create the NSX Load Balancer for vRealize Automation and vRealize Operations Manager for VMware Cloud Foundation in Region B

The NSX load balancer used for vRealize virtual machines can not be failed over, as such one must be configured in Region B to support the load balancing requirements of these applications.

Procedure

- 1 [Deploy the NSX Edge for Load Balancing vRealize Automation and vRealize Operations Manager for VMware Cloud Foundation in Region B](#)

Deploy a load balancer for use by the management applications connected to the application virtual network Mgmt-xRegion01-VXLAN after their failover to Region B.

- 2 [Disable the Interface on the vRealize NSX Edge Load Balancer for VMware Cloud Foundation in Region B](#)

Because the load balancers in Region A and Region B have the same IP addresses, the load balancer in Region B must have its interface disconnected until a disaster recovery event occurs.

- 3 [Configure the NSX Load Balancer for vRealize Automation and vRealize Operations Manager for VMware Cloud Foundation in Region B](#)

Configure the NSX Edge to perform load balancing for vRealize Automation and vRealize Operations Manager when those applications are running in Region B.

Deploy the NSX Edge for Load Balancing vRealize Automation and vRealize Operations Manager for VMware Cloud Foundation in Region B

Deploy a load balancer for use by the management applications connected to the application virtual network Mgmt-xRegion01-VXLAN after their failover to Region B.

Procedure

- 1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Settings	Value
URL	https://lax01m01vc01.lax01.rainpole.local/ui
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Networking and security** inventory, click **NSX Edges**.
- 3 From the **NSX Manager** drop-down menu, select **172.17.11.65**
- 4 Click **Add** and select **Edge Services Gateway**.

The **New Edge Services Gateway** wizard opens.

5 On the **Basic details** page, configure the settings and click **Next**.

Setting	Value
Name	lax01m01lb01
Deploy Edge Appliance VM	Selected
High Availability	Selected

6 On the **Settings** page, configure the settings, and click **Next**.

Setting	Value
User name	admin
Password	<i>edge_admin_password</i>
SSH access	Enabled
FIPS mode	Disabled
Auto rule generation	Enabled
Edge Control Level logging	INFO

7 On the **Deployment configuration** page, add two NSX Edge appliances with the following configuration, and click **Next**.

Setting	Value
Data center	lax01-m01dc
Appliance size	Large <ul style="list-style-type: none"> ■ vCPUs 2 ■ Memory 1GB
Cluster / Resource pool	lax01-m01-mgmt01
Datastore	lax01-m01-vsan01
Folder	Networking VMs
Resource reservation	System managed

8 On the **Interface** page, click **Add**, configure the settings, click **OK**, and click **Next**.

Setting	Value
Name	mgmt-vnic-vrealize-edge
Type	Internal
Connected to	Mgmt-xRegion01-VXLAN
Connectivity status	Connected
Primary IP address	Same as sfo01m01lb01 in Region A
Secondary IP address	Same as sfo01m01lb01 in Region A
Subnet prefix length	Same as sfo01m01lb01 in Region A

Setting	Value
MTU	9000
Send ICMP Redirect	Selected

9 On the **Default gateway** page, enter **192.168.11.1** for **Gateway IP** and click **Next**.

10 On the **Firewall default policy** page, configure the settings and click **Next**.

Setting	Value
Firewall default policy	Enabled
Default traffic policy	Allow
Logging	Disabled

11 On the **High availability** page, configure the settings and click **Next**.

Setting	Value
vNIC	any
Declare dead time	15
HA Logging	Enabled
Log level	Info

12 On the **Review** page, review the configuration settings you entered and click **Finish**.

Disable the Interface on the vRealize NSX Edge Load Balancer for VMware Cloud Foundation in Region B

Because the load balancers in Region A and Region B have the same IP addresses, the load balancer in Region B must have its interface disconnected until a disaster recovery event occurs.

Procedure

1 In a Web browser, log in to the Compute vCenter Server by using the vSphere Client.

Settings	Value
URL	https://lax01w01vc01.lax01.rainpole.local/ui
User name	administrator@vsphere.local
Password	<i>vsphere_admin_password</i>

2 In the **Networking and security** inventory, click **NSX Edges**.

3 From the **NSX Manager** drop-down menu, select **172.17.11.65**.

4 Click the link of the **lax01m01lb01** Edge device.

5 On the NSX Edges page, click **Configure** tab.

6 Click **Interfaces**, select the **mgmt-vnic-vrealize-edge** vNIC, and click **Edit**.

- 7 In the **Edit NSX Edge interface** dialog box, set **Connectivity status** to *Disconnected* and click **OK**.

Configure the NSX Load Balancer for vRealize Automation and vRealize Operations Manager for VMware Cloud Foundation in Region B

Configure the NSX Edge to perform load balancing for vRealize Automation and vRealize Operations Manager when those applications are running in Region B.

Prerequisites

Ensure that SSL passthrough for vRealize Operations Manager is configured on the NSX Load balancer in Region A. See *Configure SSL Passthrough for vRealize Operations Manager* in the *VMware Cloud Foundation Operations and Administration Guide*.

Procedure

- 1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Setting	Value
URL	https://sfo01m01vc01.sfo01.rainpole.local/ui
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Get the *edge-id* for the sfo01m01lb01 load balancer in Region A.
- In the **Networking and security** inventory, click **NSX Edges**.
 - From the **NSX Manager** drop-down menu, select **172.16.11.65**.
 - Copy the ID listed in the **ID** field for the sfo01m01lb01 Edge device.
- 3 Retrieve the load balancer configuration from the load balancer in Region A run by using a REST client to run the command.

```
GET https://172.16.11.65/api/4.0/edges/edge-id/loadbalancer/config
```

Sample load balancer configuration.

```
<?xml version="1.0" encoding="UTF-8"?>
<loadBalancer>
  <version>168</version>
  <enabled>true</enabled>
  <enableServiceInsertion>false</enableServiceInsertion>
  <accelerationEnabled>true</accelerationEnabled>
  <virtualServer>
    <virtualServerId>virtualServer-1</virtualServerId>
    <name>vrops-svr-443</name>
    <enabled>true</enabled>
    <ipAddress>192.168.11.35</ipAddress>
    <protocol>https</protocol>
    <port>443</port>
```

```

    <connectionLimit>0</connectionLimit>
    <defaultPoolId>pool-1</defaultPoolId>
    <applicationProfileId>applicationProfile-2</applicationProfileId>
    <enableServiceInsertion>false</enableServiceInsertion>
    <accelerationEnabled>true</accelerationEnabled>
  </virtualServer>
  <virtualServer>
    <virtualServerId>virtualServer-2</virtualServerId>
    <name>vrops-svr-80-redirect</name>
    <enabled>true</enabled>
    <ipAddress>192.168.11.35</ipAddress>
    <protocol>http</protocol>
    <port>80</port>
    <connectionLimit>0</connectionLimit>
    <applicationProfileId>applicationProfile-1</applicationProfileId>
    <enableServiceInsertion>false</enableServiceInsertion>
    <accelerationEnabled>true</accelerationEnabled>
  </virtualServer>
  <virtualServer>
    <virtualServerId>virtualServer-23</virtualServerId>
    <name>vra-svr-443</name>
    <description>vRealize Automation Appliance UI</description>
    <enabled>true</enabled>
    <ipAddress>192.168.11.53</ipAddress>
    <protocol>https</protocol>
    <port>443</port>
    <connectionLimit>0</connectionLimit>
    <defaultPoolId>pool-22</defaultPoolId>
    <applicationProfileId>applicationProfile-11</applicationProfileId>
    <enableServiceInsertion>false</enableServiceInsertion>
    <accelerationEnabled>false</accelerationEnabled>
  </virtualServer>
  <virtualServer>
    <virtualServerId>virtualServer-24</virtualServerId>
    <name>vra-svr-8444</name>
    <description>vRealize Automation Remote Console Proxy</description>
    <enabled>true</enabled>
    <ipAddress>192.168.11.53</ipAddress>
    <protocol>https</protocol>
    <port>8444</port>
    <connectionLimit>0</connectionLimit>
    <defaultPoolId>pool-23</defaultPoolId>
    <applicationProfileId>applicationProfile-11</applicationProfileId>
    <enableServiceInsertion>false</enableServiceInsertion>
    <accelerationEnabled>false</accelerationEnabled>
  </virtualServer>
  <virtualServer>
    <virtualServerId>virtualServer-25</virtualServerId>
    <name>vra-vro-8283</name>
    <description>vRealize Orchestrator Control Center</description>
    <enabled>true</enabled>
    <ipAddress>192.168.11.53</ipAddress>
    <protocol>https</protocol>
    <port>8283</port>
    <connectionLimit>0</connectionLimit>

```

```

    <defaultPoolId>pool-24</defaultPoolId>
    <applicationProfileId>applicationProfile-11</applicationProfileId>
    <enableServiceInsertion>false</enableServiceInsertion>
    <accelerationEnabled>false</accelerationEnabled>
  </virtualServer>
  <virtualServer>
    <virtualServerId>virtualServer-26</virtualServerId>
    <name>vra-iws-443</name>
    <description>vRealize Automation IaaS Web UI</description>
    <enabled>true</enabled>
    <ipAddress>192.168.11.56</ipAddress>
    <protocol>https</protocol>
    <port>443</port>
    <connectionLimit>0</connectionLimit>
    <defaultPoolId>pool-25</defaultPoolId>
    <applicationProfileId>applicationProfile-11</applicationProfileId>
    <enableServiceInsertion>false</enableServiceInsertion>
    <accelerationEnabled>false</accelerationEnabled>
  </virtualServer>
  <virtualServer>
    <virtualServerId>virtualServer-27</virtualServerId>
    <name>vra-ims-443</name>
    <description>vRealize Automation IaaS Manager</description>
    <enabled>true</enabled>
    <ipAddress>192.168.11.59</ipAddress>
    <protocol>https</protocol>
    <port>443</port>
    <connectionLimit>0</connectionLimit>
    <defaultPoolId>pool-26</defaultPoolId>
    <applicationProfileId>applicationProfile-12</applicationProfileId>
    <enableServiceInsertion>false</enableServiceInsertion>
    <accelerationEnabled>false</accelerationEnabled>
  </virtualServer>
  <pool>
    <poolId>pool-23</poolId>
    <name>vra-svr-8444</name>
    <algorithm>leastconn</algorithm>
    <transparent>false</transparent>
    <monitorId>monitor-23</monitorId>
    <member>
      <memberId>member-72</memberId>
      <ipAddress>192.168.11.51</ipAddress>
      <weight>1</weight>
      <monitorPort>443</monitorPort>
      <port>8444</port>
      <maxConn>0</maxConn>
      <minConn>0</minConn>
      <condition>enabled</condition>
      <name>vra01svr01a</name>
    </member>
    <member>
      <memberId>member-73</memberId>
      <ipAddress>192.168.11.52</ipAddress>
      <weight>1</weight>
      <monitorPort>443</monitorPort>

```

```

    <port>8444</port>
    <maxConn>0</maxConn>
    <minConn>0</minConn>
    <condition>enabled</condition>
    <name>vra01svr01b</name>
  </member>
  <member>
    <memberId>member-74</memberId>
    <ipAddress>192.168.11.50</ipAddress>
    <weight>1</weight>
    <monitorPort>443</monitorPort>
    <port>8444</port>
    <maxConn>0</maxConn>
    <minConn>0</minConn>
    <condition>enabled</condition>
    <name>vra01svr01c</name>
  </member>
</pool>
<pool>
  <poolId>pool-24</poolId>
  <name>vra-vro-8283</name>
  <algorithm>leastconn</algorithm>
  <transparent>false</transparent>
  <monitorId>monitor-24</monitorId>
  <member>
    <memberId>member-75</memberId>
    <ipAddress>192.168.11.51</ipAddress>
    <weight>1</weight>
    <monitorPort>8283</monitorPort>
    <port>8283</port>
    <maxConn>0</maxConn>
    <minConn>0</minConn>
    <condition>enabled</condition>
    <name>vra01svr01a</name>
  </member>
  <member>
    <memberId>member-76</memberId>
    <ipAddress>192.168.11.52</ipAddress>
    <weight>1</weight>
    <monitorPort>8283</monitorPort>
    <port>8283</port>
    <maxConn>0</maxConn>
    <minConn>0</minConn>
    <condition>enabled</condition>
    <name>vra01svr01b</name>
  </member>
  <member>
    <memberId>member-77</memberId>
    <ipAddress>192.168.11.50</ipAddress>
    <weight>1</weight>
    <monitorPort>8283</monitorPort>
    <port>8283</port>
    <maxConn>0</maxConn>
    <minConn>0</minConn>
    <condition>enabled</condition>

```

```

    <name>vra01svr01c</name>
  </member>
</pool>
<pool>
  <poolId>pool-25</poolId>
  <name>vra-iws-443</name>
  <algorithm>leastconn</algorithm>
  <transparent>>false</transparent>
  <monitorId>monitor-22</monitorId>
  <member>
    <memberId>member-78</memberId>
    <ipAddress>192.168.11.54</ipAddress>
    <weight>1</weight>
    <monitorPort>443</monitorPort>
    <port>443</port>
    <maxConn>0</maxConn>
    <minConn>0</minConn>
    <condition>enabled</condition>
    <name>vra01iws01a</name>
  </member>
  <member>
    <memberId>member-79</memberId>
    <ipAddress>192.168.11.55</ipAddress>
    <weight>1</weight>
    <monitorPort>443</monitorPort>
    <port>443</port>
    <maxConn>0</maxConn>
    <minConn>0</minConn>
    <condition>enabled</condition>
    <name>vra01iws01b</name>
  </member>
</pool>
<pool>
  <poolId>pool-26</poolId>
  <name>vra-ims-443</name>
  <algorithm>leastconn</algorithm>
  <transparent>>false</transparent>
  <monitorId>monitor-21</monitorId>
  <member>
    <memberId>member-80</memberId>
    <ipAddress>192.168.11.57</ipAddress>
    <weight>1</weight>
    <monitorPort>443</monitorPort>
    <port>443</port>
    <maxConn>0</maxConn>
    <minConn>0</minConn>
    <condition>enabled</condition>
    <name>vra01ims01a</name>
  </member>
  <member>
    <memberId>member-81</memberId>
    <ipAddress>192.168.11.58</ipAddress>
    <weight>1</weight>
    <monitorPort>443</monitorPort>
    <port>443</port>

```

```

    <maxConn>0</maxConn>
    <minConn>0</minConn>
    <condition>enabled</condition>
    <name>vra01ims01b</name>
  </member>
</pool>
<pool>
  <poolId>pool-22</poolId>
  <name>vra-svr-443</name>
  <ipVersionFilter>any</ipVersionFilter>
  <algorithm>leastconn</algorithm>
  <transparent>>false</transparent>
  <monitorId>monitor-23</monitorId>
  <member>
    <memberId>member-69</memberId>
    <ipAddress>192.168.11.51</ipAddress>
    <weight>1</weight>
    <monitorPort>443</monitorPort>
    <maxConn>0</maxConn>
    <minConn>0</minConn>
    <condition>enabled</condition>
    <name>vra01svr01a</name>
  </member>
  <member>
    <memberId>member-82</memberId>
    <ipAddress>192.168.11.52</ipAddress>
    <weight>1</weight>
    <monitorPort>443</monitorPort>
    <maxConn>0</maxConn>
    <minConn>0</minConn>
    <condition>enabled</condition>
    <name>vra01svr01b</name>
  </member>
  <member>
    <memberId>member-83</memberId>
    <ipAddress>192.168.11.50</ipAddress>
    <weight>1</weight>
    <monitorPort>443</monitorPort>
    <maxConn>0</maxConn>
    <minConn>0</minConn>
    <condition>enabled</condition>
    <name>vra01svr01c</name>
  </member>
</pool>
<pool>
  <poolId>pool-1</poolId>
  <name>vrops-svr-443</name>
  <algorithm>leastconn</algorithm>
  <transparent>>false</transparent>
  <monitorId>monitor-4</monitorId>
  <member>
    <memberId>member-84</memberId>
    <ipAddress>192.168.11.31</ipAddress>
    <weight>1</weight>
    <monitorPort>443</monitorPort>

```

```

    <port>443</port>
    <maxConn>10</maxConn>
    <minConn>10</minConn>
    <condition>enabled</condition>
    <name>vrops01svr01a</name>
  </member>
  <member>
    <memberId>member-85</memberId>
    <ipAddress>192.168.11.32</ipAddress>
    <weight>1</weight>
    <monitorPort>443</monitorPort>
    <port>443</port>
    <maxConn>10</maxConn>
    <minConn>10</minConn>
    <condition>enabled</condition>
    <name>vrops01svr01b</name>
  </member>
  <member>
    <memberId>member-86</memberId>
    <ipAddress>192.168.11.33</ipAddress>
    <weight>1</weight>
    <monitorPort>443</monitorPort>
    <port>443</port>
    <maxConn>10</maxConn>
    <minConn>10</minConn>
    <condition>enabled</condition>
    <name>vrops01svr01c</name>
  </member>
  <member>
    <memberId>member-87</memberId>
    <ipAddress>192.168.11.34</ipAddress>
    <weight>1</weight>
    <monitorPort>443</monitorPort>
    <port>443</port>
    <maxConn>10</maxConn>
    <minConn>10</minConn>
    <condition>enabled</condition>
    <name>vrops01svr01d</name>
  </member>
</pool>
<applicationProfile>
  <applicationProfileId>applicationProfile-1</applicationProfileId>
  <persistence>
    <method>sourceip</method>
    <expire>1800</expire>
  </persistence>
  <name>vrops-http-redirect</name>
  <insertXForwardedFor>false</insertXForwardedFor>
  <sslPassthrough>false</sslPassthrough>
  <template>HTTP</template>
  <serverSslEnabled>false</serverSslEnabled>
  <httpRedirect>
    <to>https://192.168.11.35/vcops-web-ent/login.action</to>
  </httpRedirect>
</applicationProfile>

```

```

<applicationProfile>
  <applicationProfileId>applicationProfile-11</applicationProfileId>
  <persistence>
    <method>sourceip</method>
    <expire>1800</expire>
  </persistence>
  <name>vra-https-persist</name>
  <insertXForwardedFor>false</insertXForwardedFor>
  <sslPassthrough>true</sslPassthrough>
  <template>HTTPS</template>
  <serverSslEnabled>false</serverSslEnabled>
</applicationProfile>
<applicationProfile>
  <applicationProfileId>applicationProfile-12</applicationProfileId>
  <name>vra-https</name>
  <insertXForwardedFor>false</insertXForwardedFor>
  <sslPassthrough>true</sslPassthrough>
  <template>HTTPS</template>
  <serverSslEnabled>false</serverSslEnabled>
</applicationProfile>
<applicationProfile>
  <applicationProfileId>applicationProfile-2</applicationProfileId>
  <persistence>
    <method>sourceip</method>
    <expire>1800</expire>
  </persistence>
  <name>vrops-https</name>
  <insertXForwardedFor>false</insertXForwardedFor>
  <sslPassthrough>true</sslPassthrough>
  <template>HTTPS</template>
  <serverSslEnabled>false</serverSslEnabled>
</applicationProfile>
<monitor>
  <monitorId>monitor-1</monitorId>
  <type>tcp</type>
  <interval>5</interval>
  <timeout>15</timeout>
  <maxRetries>3</maxRetries>
  <name>default_tcp_monitor</name>
</monitor>
<monitor>
  <monitorId>monitor-2</monitorId>
  <type>http</type>
  <interval>5</interval>
  <timeout>15</timeout>
  <maxRetries>3</maxRetries>
  <method>GET</method>
  <url>/</url>
  <name>default_http_monitor</name>
</monitor>
<monitor>
  <monitorId>monitor-3</monitorId>
  <type>https</type>
  <interval>5</interval>
  <timeout>15</timeout>

```

```

    <maxRetries>3</maxRetries>
    <method>GET</method>
    <url>/</url>
    <name>default_https_monitor</name>
</monitor>
<monitor>
  <monitorId>monitor-4</monitorId>
  <type>https</type>
  <interval>5</interval>
  <timeout>16</timeout>
  <maxRetries>3</maxRetries>
  <method>GET</method>
  <url>/suite-api/api/deployment/node/status</url>
  <name>vrops-443-monitor</name>
  <receive>ONLINE</receive>
</monitor>
<monitor>
  <monitorId>monitor-21</monitorId>
  <type>https</type>
  <interval>3</interval>
  <timeout>10</timeout>
  <maxRetries>3</maxRetries>
  <method>GET</method>
  <url>/VMPSProvision</url>
  <name>vra-ims-443-monitor</name>
  <receive>ProvisionService</receive>
</monitor>
<monitor>
  <monitorId>monitor-22</monitorId>
  <type>https</type>
  <interval>3</interval>
  <timeout>10</timeout>
  <maxRetries>3</maxRetries>
  <method>GET</method>
  <url>/wapi/api/status/web</url>
  <name>vra-iws-443-monitor</name>
  <receive>REGISTERED</receive>
</monitor>
<monitor>
  <monitorId>monitor-23</monitorId>
  <type>https</type>
  <interval>3</interval>
  <timeout>10</timeout>
  <maxRetries>3</maxRetries>
  <method>GET</method>
  <url>/vcac/services/api/health</url>
  <expected>204</expected>
  <name>vra-svr-443-monitor</name>
</monitor>
<monitor>
  <monitorId>monitor-24</monitorId>
  <type>https</type>
  <interval>3</interval>
  <timeout>10</timeout>
  <maxRetries>3</maxRetries>

```

```

    <method>GET</method>
    <url>/vco-controlcenter/docs</url>
    <name>vra-vro-8283-monitor</name>
  </monitor>
  <logging>
    <enable>true</enable>
    <logLevel>info</logLevel>
  </logging>
</loadBalancer>

```

- 4 To later configure the load balancer in Region B, save the output to a file.
 - a Edit the file and remove the line that begins with `<version>`.
 - b Save the file.
- 5 In a Web browser, log in to vCenter Server by using the vSphere Client.

Settings	Value
URL	https://lax01m01vc01.lax01.rainpole.local/ui
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 6 Get the *edge-id* for the lax01m01lb01 load balancer in Region A.
 - a In the **Networking and security** inventory, click **NSX Edges**.
 - b From the **NSX Manager** drop-down menu, select **172.17.11.65**.
 - c Copy the ID listed in the **ID** field for the lax01m01lb01 Edge device.
- 7 Use a REST client to configure the vRealize Edge load balancer in Region B.
 - a In a REST client, run the following command.

```
PUT https://172.17.11.65/api/4.0/edges/edge-id/loadbalancer/config
```

- b Paste the output that you saved in a file, from the load balancer configuration in Region A, in the body of the PUT request.

You receive a status code of 204 No Content as confirmation the command was successful.

Update Universal Logical Switch information on the SDDC manager for VMware Cloud Foundation in Region B

When configuring the environment for disaster recovery, the universal logical switch that is created in Region A is made available in region B and the virtual machines of vRealize Log Insight are moved to a different port group. You must update the SDDC Manager database in Region B to maintain connectivity for the virtual machines. You perform these steps in SDDC Manager in Region B only.

Procedure

- 1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Setting	Value
URL	https://sfo01m01vc01.sfo01.rainpole.local/ui
User name	administrator@vsphere.local
Password	<i>vsphere_admin_password</i>

- 2 Get the port group name for each Application Virtual Network.
 - a In the **Networking** inventory, expand the **sfo01m01vc01.sfo01.rainpole.local** tree and expand the **sfo01-m01dc** data center.
 - b Select the **sfo01-m01-vds01** distributed switch, click the **Networks** tab, and click **Distributed port groups**.
 - c Locate the port group name for each Application Virtual Network and save the entries.

Application Virtual Network	Port Group Name
Mgmt-xRegion01-VXLAN	vxx-dvs-xxxx-Mgmt-xRegion01-VXLAN
Mgmt-RegionB01-VXLAN	vxx-dvs-xxxx-Mgmt-RegionB01-VXLAN

- 3 Get the name of the UDLR.
 - a In the **Networking and security** inventory, click **NSX Edges**.
 - b From the **NSX Manager** drop-down menu, select **172.16.11.65**.
 - c Locate the name of the sfo01m01udlr01 UDLR and write down the entry.
- 4 Log in to SDDC Manager by using a Secure Shell (SSH) client.

Setting	Value
FQDN	lax01m01sddcmgr.lax01.rainpole.local
User name	vcf
Password	<i>vcf_user_password</i>

- 5 Create a backup dump of the platform database as the root user by running the command.

```
su -pg_dump --host=localhost -U postgres platform > platform.bak
```

- 6 Login to platform database.

```
psql -h localhost -U postgres -d platform
```

- 7 Verify the current status of the AVN table by running the following command

```
SELECT * FROM avn;
```

- 8 Update the port group name for the Mgmt-xRegion01-VXLAN Application Virtual Network in SDDC Manager by using the entry you previously saved.

```
update avn SET portgroup_name = 'vxw-dvs-xxxx-Mgmt-xRegion01-VXLAN' WHERE name = 'Mgmt-xRegion01-VXLAN';
```

- 9 Update the port group and UDLR name for the Mgmt-RegionB01-VXLAN Application Virtual Network in SDDC Manager by using the entries you previously saved.

```
update avn SET name = 'Mgmt-RegionB01-VXLAN' WHERE name = 'Mgmt-RegionA01-VXLAN';
update avn SET portgroup_name = 'vxw-dvs-xxxx-Mgmt-RegionB01-VXLAN' WHERE name = 'Mgmt-RegionB01-VXLAN';
update avn set region_type = 'REGION_B' WHERE name = 'Mgmt-RegionB01-VXLAN';
update avn set router_name = 'm01udlr01' WHERE name = 'Mgmt-RegionB01-VXLAN';
```

- 10 Verify that the values are updated and exit the platform database.

```
SELECT * FROM avn;
\q
```

Deploy and Configure vSphere Replication for VMware Cloud Foundation

5

You deploy and configure vSphere Replication to enable replication of critical virtual machine data from Region A to Region B for failover by using Site Recovery Manager in the cases of disaster or planned migration.

Procedure

- 1 Prerequisites for the vSphere Replication Deployment for VMware Cloud Foundation in Region A**
To deploy a new vSphere Replication virtual appliance, your environment must satisfy certain hardware and software requirements.
- 2 Deploy vSphere Replication for VMware Cloud Foundation in Region A**
Deploy vSphere Replication to enable replication of virtual machines between the protected and the recovery regions.
- 3 Deploy vSphere Replication for VMware Cloud Foundation in Region B**
After you deploy vSphere Replication in Region A, deploy it in Region B to complete the support for replication of virtual machines between the two regions.
- 4 Connect the vSphere Replication Instances for VMware Cloud Foundation**
To use vSphere Replication between Region A and Region B, you must configure a connection between the two vSphere Replication appliances because each region is managed by a different vCenter Server instance.
- 5 Isolate Network Traffic of vSphere Replication for VMware Cloud Foundation**
vSphere Replication can consume a lot of bandwidth during initial replication, and when virtual machines are added or destroyed. To avoid network problems in the data center, isolate replication traffic from other network traffic. Isolating the vSphere Replication traffic also enhances network performance in the data center by reducing the impact of this traffic on other traffic types.

Prerequisites for the vSphere Replication Deployment for VMware Cloud Foundation in Region A

To deploy a new vSphere Replication virtual appliance, your environment must satisfy certain hardware and software requirements.

Software Requirements

Before you install vSphere Replication, make sure that you have the following configuration available in your environment.

Component	Requirement
Installation package	Download the vSphere Replication VMware–vSphere_Replication–8.2.0– <i>build_number</i> .iso image and mount it on the machine that you use to access the vSphere Client.
Certificate Authority	<ul style="list-style-type: none"> ■ Configure the root Active Directory domain controller as a certificate authority for the environment. ■ Download the CertGenVVD tool and generate the signed certificate for vSphere Replication. See the <i>VMware Validated Design Planning and Preparation</i> documentation.

IP Addresses, Host Names, and Network Configuration

Allocate a temporary static IP address and use the existing network configuration for the new vSphere Replication appliance deployment.

Table 5-1. Network Configuration of vSphere Replication in Region A

Setting	Value
Host name	sfo01m01vrms01
Static IPv4 address	172.16.11.123
Subnet mask	255.255.255.0
Default gateway	172.16.11.253
DNS servers	172.16.11.5,172.16.11.4
FQDN	sfo01m01vrms01.sfo01.rainpole.local
Used ports	5480
NTP servers	<ul style="list-style-type: none"> ■ ntp.sfo01.rainpole.local ■ ntp.lax01.rainpole.local
Management Network Port Group	sfo01-m01-vds01-management
Replication Traffic Port Group	sfo01-m01-vds01-replication

Table 5-2. Network Configuration of vSphere Replication in Region B

Setting	Value
Host name	lax01m01vrms01
Static IPv4 address	172.17.11.123
Subnet mask	255.255.255.0
Default gateway	172.17.11.253
DNS servers	172.17.11.5,172.17.11.4

Table 5-2. Network Configuration of vSphere Replication in Region B (continued)

Setting	Value
FQDN	lax01m01vrms01.lax01.rainpole.local
Used ports	5480
NTP servers	<ul style="list-style-type: none"> ■ ntp.lax01.rainpole.local ■ ntp.sfo01.rainpole.local
Management Network Port Group	lax01-m01-vds01-management
Replication Traffic Port Group	lax01-m01-vds01-replication

Table 5-3. VLAN and IP Requirements for vSphere Replication Traffic

Requirement	Value for Region A	Value for Region B
VLAN ID	1616	1716
Static IPv4 address	172.16.16.71	172.17.16.71
Subnet mask	255.255.255.0	255.255.255.0
Gateway	172.16.16.253	172.17.16.253

Deploy vSphere Replication for VMware Cloud Foundation in Region A

Deploy vSphere Replication to enable replication of virtual machines between the protected and the recovery regions.

Deploy vSphere Replication for VMware Cloud Foundation in Region A

Deploy the new vSphere Replication appliance in the protected region.

Procedure

- 1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Setting	Value
URL	https://sfo01m01vc01.sfo01.rainpole.local/ui
User name	administrator@vsphere.local
Password	<i>vsphere_admin_password</i>

- 2 In the **Hosts and clusters** inventory, expand the **sfo01m01vc01.sfo01.rainpole.local** tree and expand the **sfo01-m01dc** data center.

3 Deploy the new vSphere Replication appliance.

- a Right-click the **sfo01-m01-mgmt01** cluster and select **Deploy OVF template**.
- b On the **Select an OVF template** page, select **Local file**, click **Choose files**, use a multiple selection to select the following files from the bin folder of the .iso mount for vSphere Replication, click **Open**, and click **Next**.
 - vSphere_Replication_OVF10.ovf
 - vSphere_Replication-support.vmdk
 - vSphere_Replication-system.vmdk
- c On the **Select a name and folder** page, configure the settings and click **Next**.

Setting	Value
Name	sfo01m01vrms01
vCenter Server	sfo01m01vc01.sfo01.rainpole.local
Data center	sfo01-m01dc
Folder	Management VMs

- d On the **Select a compute resource** page, select the **sfo01-m01-mgmt01** cluster and click **Next**.
- e On the **Review details** page, click **Next**.
- f On the **License agreements** page, accept the license agreement and click **Next**.
- g On the **Configuration** page, leave the default **4 vCPU** configuration selected and click **Next**.
- h On the **Select storage** page, configure the settings and click **Next**.

Setting	Value
Select virtual disk format	Thin provision
VM Storage Policy	vSAN Default Storage Policy
Datastore	sfo01-m01-vsant01

- i On the **Select networks** page, configure the settings and click **Next**.

Setting	Value
Destination network	sfo01-m01-vds01-management
IP allocation	Static - Manual
IP protocol	IPv4

- j On the **Customize template** page, configure the settings and click **Next**.

Setting	Value
Password	<i>vr_sfo_root_password</i>
Confirm password	<i>vr_sfo_root_password</i>
NTP Servers	ntp.sfo01.rainpole.local,ntp.lax01.rainpole.local
Hostname	sfo01m01vrms01.sfo01.rainpole.local
Default Gateway	172.16.11.253
Domain Name	sfo01.rainpole.local
Domain Search Path	sfo01.rainpole.local
Domain Name Servers	172.16.11.5,172.16.11.4
Management Network IP Address	172.16.11.123
Management Network Netmask	255.255.255.0

- k On the **vService bindings** page, click **Next**.
- l On the **Ready to complete** page, click **Finish**.

Wait for the deployment to complete.

- 4 Right-click the **sfo01m01vrms01** virtual machine, and select **Power > Power on**.

Replace the Certificate of vSphere Replication for VMware Cloud Foundation in Region A

Replace the certificates on VMware vSphere Replication in Region A so that vSphere Replication can communicate with connected management solutions over a secure connection.

Table 5-4. PKCS#12 Files for vSphere Replication in Region A

vSphere Replication	Certificate File
sfo01m01vrms01.sfo01.rainpole.local	sfo01m01vrms01.5.p12

Procedure

- 1 In a Web browser, log in to vSphere Replication by using the Virtual Appliance Management Interface (VAMI).

Setting	Value
URL	https://sfo01m01vrms01.sfo01.rainpole.local:5480
User name	root
Password	<i>vr_sfo_root_password</i>

- 2 Upload and install the new certificate.
 - a On the **VR** tab, click the **Configuration** tab.
 - b In the **SSL certificate policy** section, next to **Upload PKCS#12 (*.pfx) file**, click **Choose file**, and browse to the `sfo01m01vrms01.5.p12` file.
 - c Click **Upload and install**.
 - d Enter the certificate password when prompted and click **OK**.

After you upload and apply the SSL certificate, the VAMI session closes.

- 3 Log back in to vSphere Replication by using the Virtual Appliance Management Interface (VAMI).

Setting	Value
User name	root
Password	<i>vr_sfo_root_password</i>

- 4 On the **VR** tab, click the **Security** tab.
- 5 Verify that the **Current SSL Certificate** section shows the updated certificate information.

Register vSphere Replication with vCenter Single Sign-On for VMware Cloud Foundation in Region A

After you deploy the vSphere Replication appliance in the protected region, register vSphere Replication with the Platform Services Controller pair by using the vSphere Replication appliance management interface.

Procedure

- 1 In a Web browser, log in to vSphere Replication by using the Virtual Appliance Management Interface (VAMI).

Setting	Value
URL	<code>https://sfo01m01vrms01.sfo01.rainpole.local:5480</code>
User name	root
Password	<i>vr_sfo_root_password</i>

- 2 On the **VR** tab, click **Configuration**, configure the settings, and click **Save and restart service**.

Setting	Value
Configuration Mode	Configure using the embedded database
LookupService Address	<code>sfo01m01psc01.sfo01.rainpole.local</code>
SSO Administrator	<code>administrator@vsphere.local</code>
Password	<i>vsphere_admin_password</i>
VRM Host	<code>sfo01m01vrms01.sfo01.rainpole.local</code>
VRM Site Name	<code>sfo01m01vc01.sfo01.rainpole.local</code>

Setting	Value
vCenter Server Address	sfo01m01vc01.sfo01.rainpole.local
vCenter Server Port	80
vCenter Server Admin Mail	<i>vcenter_server_admin_email</i>

3 In the **Confirm SSL certificate** dialog box, click **Accept**.

Wait until the vSphere Replication services are restarted.

4 Under **Service Status**, verify that the status of the vSphere Replication service is running.

Deploy vSphere Replication for VMware Cloud Foundation in Region B

After you deploy vSphere Replication in Region A, deploy it in Region B to complete the support for replication of virtual machines between the two regions.

Deploy the vSphere Replication Appliance for VMware Cloud Foundation in Region B

After you deploy vSphere Replication on the protected region, deploy the vSphere Replication appliance on the recovery region to complete replication deployment.

Procedure

1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Settings	Value
URL	https://lax01m01vc01.lax01.rainpole.local/ui
User name	administrator@vsphere.local
Password	<i>vsphere_admin_password</i>

2 In the **Hosts and clusters** inventory, expand the **lax01m01vc01.lax01.rainpole.local** tree and expand the **lax01-m01dc** data center.

3 Deploy the new vSphere Replication appliance.

a Right-click the **lax01-m01-mgmt01** cluster and select **Deploy OVF template**.

b On the **Select an OVF template** page, select **Local file**, click **Choose files**, use a multiple selection to select the following files from the bin folder of the .iso mount for Site Recovery Manager, click **Open**, and click **Next**.

- vSphere_Replication_OVF10.ovf
- vSphere_Replication-support.vmdk
- vSphere_Replication-system.vmdk

- c On the **Select a name and folder** page, configure the settings and click **Next**.

Setting	Value
Name	lax01m01vrms01
vCenter Server	lax01m01vc01.lax01.rainpole.local
Data center	lax01-m01dc
Folder	Management VMs

- d On the **Select a compute resource** page, select the **lax01-m01-mgmt01** cluster and click **Next**.

- e On the **Review details** page, click **Next**.

- f On the **License agreements** page, accept the license agreement and click **Next**.

- g On the **Configuration** page, leave the default **4 vCPU** configuration selected and click **Next**.

- h On the **Select storage** page, configure the settings and click **Next**.

Setting	Value
Select virtual disk format	Thin provision
VM Storage Policy	vSAN Default Storage Policy
Datastore	lax01-m01-vsan01

- i On the **Select networks** page, configure the settings and click **Next**.

Setting	Value
Destination network	lax01-m01-vds01-management
IP allocation	Static - Manual
IP protocol	IPv4

- j On the **Customize template** page, configure the settings and click **Next**.

Setting	Value
Password	<i>vr_lax_root_password</i>
Confirm password	<i>vr_lax_root_password</i>
NTP Servers	ntp.lax01.rainpole.localntp.sfo01.rainpole.local,
Hostname	lax01m01vrms01.lax01.rainpole.local
Default Gateway	172.17.11.253
Domain Name	lax01.rainpole.local
Domain Search Path	lax01.rainpole.local
Domain Name Servers	172.17.11.5,172.17.11.4
Management Network IP Address	172.17.11.123
Management Network Netmask	255.255.255.0

- k On the **vService bindings** page, click **Next**.
- l On the **Ready to complete** page, click **Finish**.

Wait for the deployment to complete.

- 4 Right-click the **lax01m01vrms01** virtual machine, and select **Power > Power on**.

Replace the Certificate of vSphere Replication for VMware Cloud Foundation in Region B

Replace the certificate of vSphere Replication to reestablish secure communication with connected management solutions.

Table 5-5. PKCS#12 Files for vSphere Replication in Region B

vSphere Replication	Certificate File
lax01m01vrms01.lax01.rainpole.local	lax01m01vrms01.5.p12

Procedure

- 1 In a Web browser, log in to vSphere Replication by using the Virtual Appliance Management Interface (VAMI).

Setting	Value
URL	https://lax01m01vrms01.lax01.rainpole.local:5480
User name	root
Password	<i>vr_lax_root_password</i>

- 2 Upload and install the new certificate.
 - a On the **VR** tab, click the **Configuration** tab.
 - b In the **SSL certificate policy** section, next to **Upload PKCS#12 (*.pfx) file**, click **Choose file**, and browse to the `lax01m01vrms01.5.p12` file.
 - c Click **Upload and install**.
 - d Enter the certificate password when prompted and click **OK**.

After you upload and apply the SSL certificate, the VAMI session closes.

- 3 Log back in to vSphere Replication by using the Virtual Appliance Management Interface (VAMI).

Setting	Value
User name	root
Password	<i>vr_lax_root_password</i>

- 4 On the **VR** tab, click the **Security** tab.
- 5 Verify that the **Current SSL Certificate** section shows the updated certificate information.

Register vSphere Replication with vCenter Single Sign-On for VMware Cloud Foundation in Region B

After you deploy the vSphere Replication appliance in the recovery region, register vSphere Replication with the Platform Services Controller pair by using the vSphere Replication appliance management interface.

Procedure

- 1 In a Web browser, log in to vSphere Replication by using the Virtual Appliance Management Interface (VAMI).

Setting	Value
URL	https://lax01m01vrms01.lax01.rainpole.local:5480
User name	root
Password	<i>vr_lax_root_password</i>

- 2 On the **VR** tab, click **Configuration**, configure the settings, and click **Save and restart service**.

Setting	Value
Configuration Mode	Configure using the embedded database
LookupService Address	lax01m01psc01.lax01.rainpole.local
SSO Administrator	administrator@vsphere.local
Password	<i>vsphere_admin_password</i>
VRM Host	lax01m01vrms01.lax01.rainpole.local
VRM Site Name	lax01m01vc01.lax01.rainpole.local
vCenter Server Address	lax01m01vc01.lax01.rainpole.local
vCenter Server Port	80
vCenter Server Admin Mail	<i>vcenter_server_admin_email</i>

- 3 In the **Confirm SSL certificate** dialog box, click **Accept**.
Wait until the vSphere Replication services are restarted.
- 4 Under **Service Status**, verify that the status of the vSphere Replication service is running.

Connect the vSphere Replication Instances for VMware Cloud Foundation

To use vSphere Replication between Region A and Region B, you must configure a connection between the two vSphere Replication appliances because each region is managed by a different vCenter Server instance.

Procedure

- 1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Setting	Value
URL	https://sfo01m01vc01.sfo01.rainpole.local/ui
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Site Recovery** inventory, on the **sfo01m01vc01.sfo01.rainpole.local** site pane, click **Open Site Recovery**.

The **Site Recovery** page opens.

- 3 Connect the two vSphere Replication instances.

- a On the **Site Recovery** page, click **New site pair**.

The **New site pair** wizard opens.

- b On the **Site details** page, configure the settings and click **Next**.

Setting	Value
First site--> Select a local vCenter Server	sfo01m01vc01.sfo01.rainpole.local
Second site	Platform Services Controller
PSC host name	lax01m01psc01.lax01.rainpole.local
PSC port	443
User name	administrator@vsphere.local
Password	vsphere_admin_password

- c In the **Security alert** dialog box, click **Connect**.
- d On the **vCenter Server and services** page, select the **lax01m01vc01.lax01.rainpole.local** vCenter Server, select the **vSphere Replication** service, and click **Next**.
- e On the **Ready to complete** page, click **Finish** and wait until the **Paired Site** appears.
- f Click **View Details** and click **Site Pair**.
- g On the **Summary** page, verify that the local and the remote sites are **Connected**.

Isolate Network Traffic of vSphere Replication for VMware Cloud Foundation

vSphere Replication can consume a lot of bandwidth during initial replication, and when virtual machines are added or destroyed. To avoid network problems in the data center, isolate replication traffic from other network traffic. Isolating the vSphere Replication traffic also enhances network performance in the data center by reducing the impact of this traffic on other traffic types.

Create a Port Group for vSphere Replication Traffic for VMware Cloud Foundation

You isolate the network traffic to the vSphere Replication server by creating a dedicated port group for vSphere Replication traffic.

Procedure

- 1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Setting	Value
URL	https://sfo01m01vc01.sfo01.rainpole.local/ui
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Create a port group in the sfo01-m01-vds01 distributed switch for the vSphere Replication traffic.
 - a In the **Networking** inventory, expand the **sfo01m01vc01.sfo01.rainpole.local** tree and expand the **sfo01-m01dc** data center.
 - b Right-click the **sfo01-m01-vds01** distributed switch and select **Distributed port group > New distributed port group**.
The **New distributed port group** wizard opens.
 - c On the **Name and location** page, enter **sfo01-m01-vds01** as the port group name and click **Next**.
 - d On the **Configure settings** page, configure the settings and click **Next**.

Setting	Value
Port Binding	Static binding
VLAN Type	VLAN
VLAN ID	1616

- e On the **Ready to complete** page, review the configuration and click **Finish**.

- 3 Repeat the steps to create the vSphere Replication port group on the lax01-m01-vds01 distributed switch in Region B with the following values.

Setting	Value
vCenter Server URL	https://lax01m01vc01.lax01.rainpole.local/ui
Distributed switch	lax01-m01-vds01
Port group name	lax01-m01-vds01-replication
Port binding	Static binding
VLAN Type	VLAN ID
VLAN ID	1716

Add a Network Adapter and Configure Static Routes for vSphere Replication for VMware Cloud Foundation

You isolate the network traffic to the vSphere Replication Server by adding a dedicated network adapter to the vSphere Replication appliance to handle data from each management ESXi host.

By default, the vSphere Replication appliance has one virtual machine network adapter that is used by vSphere Replication for both replication traffic and by vCenter Server for virtual machine management. To isolate the replication traffic, you add a second adapter to the appliances in both regions and configure them for replication traffic.

Procedure

- 1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Setting	Value
URL	https://sfo01m01vc01.sfo01.rainpole.local/ui
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 To allow changes in the hardware configuration, shut down the vSphere Replication appliance.
 - a In the **Hosts and clusters** inventory, expand the **sfo01m01vc01.sfo01.rainpole.local** tree and expand the **sfo01-m01dc** data center.
 - b Right-click the **sfo01m01vrms01** appliance and select **Power > Shut down guest OS**.
 - c In the **Confirm guest shut down** dialog box, click **Yes** to proceed.
- 3 Add a VM network adapter to the vSphere Replication virtual appliance for replication traffic only.
 - a Right-click the **sfo01m01vrms01** virtual appliance and select **Edit settings**.
The **Edit settings** dialog box opens.
 - b On the **Virtual hardware** tab, click **Add new device** and select **Network adapter**.
 - c Expand the **New network** section, configure the settings, and click **OK**.

Setting	Value
New network	sfo01-m01-vds01-replication
Status	Connected at power on
Adapter type	VMXNET 3
Direct path I/O	Enabled

- d Right-click the **sfo01m01vrms01** virtual appliance and select **Power > Power On**.

- 4 In a Web browser, log in to vSphere Replication by using the Virtual Appliance Management Interface (VAMI).

Setting	Value
URL	https://sfo01m01vrms01.sfo01.rainpole.local:5480
User name	root
Password	<i>vr_sfo_root_password</i>

- 5 Configure the network settings of the new network adapter eth1.

- a Click the **Network** tab and click **Address**.
- b Under **eth1 info**, configure the settings and click **Save Settings**.

Setting	Value
IPv4 Address Type	Static
IPv4 Address	172.16.16.71
Netmask	255.255.255.0
IPv6 Address Type	None

- c Click the **VR** tab and click **Configuration**.
- d In the **IP Address for incoming storage traffic** text box, enter **172.16.16.71** and click **Apply network setting**.

172.16.16.71 is the IP address of the new network adapter that handles replication traffic.

- 6 Repeat the steps to reconfigure the lax01m01vrms01 vSphere Replication appliance in Region B, using the values from the following table.

Setting	Value
vSphere Replication appliance	lax01m01vrms01
New network	lax01-m01-vds01-replication
URL of vSphere Replication appliance	https://lax01m01vrms01.lax01.rainpole.local:5480
IPv4 address type	Static
IPv4 address	172.17.16.71
Netmask	255.255.255.0
IP address for incoming storage traffic	172.17.16.71

- 7 In a Web browser, log in to vCenter Server by using the vSphere Client.

Setting	Value
URL	https://sfo01m01vc01.sfo01.rainpole.local/ui
User name	administrator@vsphere.local
Password	<i>vsphere_admin_password</i>

8 On the vSphere Replication appliances, add static network routes to the hosts in the other region.

Appliance Host Name	Source Gateway	Target Network
sfo01m01vrms01.sfo01.rainpole.local	172.16.16.253	172.17.16.0/24
lax01m01vrms01.lax01.rainpole.local	172.17.16.253	172.16.16.0/24

- a In the **Hosts and clusters** inventory, expand the **sfo01m01vc01.sfo01.rainpole.local** tree and expand the **sfo01-m01dc** data center.
- b Select the **sfo01m01vrms01** virtual appliance, click the **Summary** tab, and click **Launch web console**.
- c In the **Launch console** dialog box, select **Web console**, and click **OK**.
- d Press ALT+F2 to switch to the command prompt.
- e Log in using the following credentials.

Setting	Value
User name	root
Password	vr_root_password

- f Edit the `/etc/systemd/network/10-eth1.network` file.

```
vi /etc/systemd/network/10-eth1.network
```

- g To create a route to from the recovery to the protected region, add the following text at the end of the file.

File	Value for sfo01m01vrms01	Value for lax01m01vrms01
<code>/etc/systemd/network/10-eth1.network</code>	[Route] Gateway=172.16.16.253 Destination=172.17.16.0/24	[Route] Gateway=172.17.16.253 Destination=172.16.16.0/24

- h To restart the network service, run the command.

```
systemctl restart systemd-networkd.service
```

- i To verify the routing table, run the `route -n` command.

Command	Output for sfo01m01vrms01	Output for lax01m01vrms01
<code>route -n</code>	Destination 172.17.16.0 Gateway 172.16.16.253 Iface eth1	Destination 172.16.16.0 Gateway 172.17.16.253 Iface eth1

- j Repeat the step on the vSphere Replication appliance in the other region.

Create VMkernel Adapter for vSphere Replication on the ESXi Hosts for VMware Cloud Foundation

You isolate the network traffic to the vSphere Replication Server by dedicating a VMkernel network adapter on each management ESXi host that sends data to the vSphere Replication Server.

Procedure

- 1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Setting	Value
URL	https://sfo01m01vc01.sfo01.rainpole.local/ui
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Create a VMkernel adapter for vSphere Replication on the sfo01m01esx01.sfo01.rainpole.local host.
 - a In the **Hosts and clusters** inventory, expand the **sfo01m01vc01.sfo01.rainpole.local** tree and expand the **sfo01-m01dc** data center.
 - b Expand the **sfo01-m01-mgmt01** cluster and select the first management host **sfo01m01esx01.sfo01.rainpole.local**.
 - c Click the **Configure** tab and under **Networking** select **VMkernel adapters**.
 - d Click **Add networking**.
The **Add networking** wizard opens.
 - e On the **Select connection type** page, select **VMkernel network adapter** and click **Next**.
 - f On the **Select target device** page, select **Select an existing network**, click **Browse**, select **sfo01-m01-vds01-replication**, click **OK**, and click **Next**.
 - g On the **Port properties** page, under **Available services**, select **vSphere Replication** and **vSphere Replication NFC**, and click **Next**.
 - h On the **IPv4 setting** page, select **Use static IPv4 settings**, configure the settings and click **Next**.

Setting	Value
IPv4 address	172.16.16.101
Subnet mask	255.255.255.0

- i On the **Ready to complete** page, verify the settings and click **Finish**.
- 3 Configure the MTU on the vSphere Replication VMkernel adapter.
 - a On the **VMkernel adapters** page, select the newly-created VMkernel port and click **Edit**.
 - b On the **Edit settings** page, under **VMkernel port settings**, change **MTU** to **9000** and click **OK**.

- 4 Repeat the previous steps to create VMkernel network adapters and configure MTU on the remaining management hosts.

Setting	IPv4 address	Port Group
sfo01m01esx02.sfo01.rainpole.local	172.16.16.102	sfo01-m01-vds01-replication
sfo01m01esx03.sfo01.rainpole.local	172.16.16.103	
sfo01m01esx04.sfo01.rainpole.local	172.16.16.104	

- 5 Repeat the step to create VMkernel network adapters on the hosts in Region B, using the following values.

Setting	Value
vCenter Server	lax01m01vc01.lax01.rainpole.local
Network	lax01-m01-vds01-replication
lax01m01esx01.lax01.rainpole.local	172.17.16.101
lax01m01esx02.lax01.rainpole.local	172.17.16.102
lax01m01esx03.lax01.rainpole.local	172.17.16.103
lax01m01esx04.lax01.rainpole.local	172.17.16.104

Important If you add new hosts to the management domain using SDDC Manager, you must follow this procedure to add and configure new VMkernel adapters on the hosts.

Configure Static Network Routes for VMware Cloud Foundation

You must configure the relevant static routes on each ESXi host at the source site to communicate with the target site. For replications to flow in the opposite direction, you must configure reverse routes on the ESXi hosts on the target site.

You add static routes on all hosts in the management domain in Region A and Region B.

Region	Hosts	Source Gateway	Target Network
Region A	sfo01m01esx01.sfo01.rainpole.local	172.16.16.253	172.17.16.0/24
	sfo01m01esx02.sfo01.rainpole.local		
	sfo01m01esx03.sfo01.rainpole.local		
	sfo01m01esx04.sfo01.rainpole.local		
Region B	lax01m01esx01.lax01.rainpole.local	172.17.16.253	172.16.16.0/24
	lax01m01esx02.lax01.rainpole.local		

Region	Hosts	Source Gateway	Target Network
	lax01m01esx03.lax01.rainpole.local		
	lax01m01esx03.lax01.rainpole.local		

Procedure

- 1 Log in to the ESXi host by using a Secure Shell (SSH) client.

Settings	Value
FQDN	sfo01m01esx01.sfo01.rainpole.local
User name	root
Password	<i>vcenter_server_root_password</i>

- 2 To create a route to the recovery region for the hosts in Region A or to the protected region for the hosts in Region B, run the following command.

Region	Command
Region A	<code>esxcli network ip route ipv4 add --gateway 172.16.16.253 --network 172.17.16.0/24</code>
Region B	<code>esxcli network ip route ipv4 add --gateway 172.17.16.253 --network 172.16.16.0/24</code>

- 3 Verify the routing table by running the command.

```
esxcli network ip route ipv4 list
```

- 4 Repeat this procedure for all management hosts in Region A and Region B.

Important If you add new hosts to the management domain using SDDC Manager, you must follow this procedure to configure static routes on the hosts..

Deploy and Configure Site Recovery Manager for VMware Cloud Foundation

6

You deploy Site Recovery to enable fail over of management applications from Region A to Region B in the cases of disaster or planned migration.

Procedure

- 1 Prerequisites for Installing Site Recovery Manager for VMware Cloud Foundation**
To deploy a new vSphere Replication virtual appliance, your environment must satisfy certain hardware and software requirements.
- 2 Deploy Site Recovery Manager for VMware Cloud Foundation in Region A**
Deploy the new Site Recovery Manager virtual appliance in the protected region.
- 3 Replace the Certificate of Site Recovery Manager for VMware Cloud Foundation in Region A**
- 4 Configure the Site Recovery Manager Appliance for VMware Cloud Foundation in Region A**
- 5 Deploy Site Recovery Manager for VMware Cloud Foundation in Region B**
Deploy the new Site Recovery Manager virtual appliance in the recovery region.
- 6 Replace the Certificate of Site Recovery Manager for VMware Cloud Foundation in Region B**
- 7 Configure the Site Recovery Manager Appliance for VMware Cloud Foundation in Region B**
- 8 Assign Licenses to the Site Recovery Manager Instances for VMware Cloud Foundation**
After both Site Recovery Manager Instances are deployed, assign the appropriate licensing.
- 9 Connect the Protected and Recovery Sites for VMware Cloud Foundation**
After you deploy Site Recovery Manager in the protected and the recovery regions, connect the instances to configure a site pair.
- 10 Configure Mappings between the Protected and the Recovery Regions for VMware Cloud Foundation**
Configure resource mappings between the protected and the recovery sites to enable failover of vRealize Suite Lifecycle Manager, vRealize Operations Manager, and vRealize Automation.

Prerequisites for Installing Site Recovery Manager for VMware Cloud Foundation

To deploy a new vSphere Replication virtual appliance, your environment must satisfy certain hardware and software requirements.

Software Requirements

Before you install Site Recovery Manager, make sure that you have the following configuration available in your environment.

Component	Requirement
Installation package	Download the Site Recovery Manager VMware-srm-va-8.2.0-build_number.iso image and mount it on the machine that you use to access the vSphere Web Client.
Certificate Authority	<ul style="list-style-type: none"> ■ Configure the root Active Directory domain controller as a certificate authority for the environment. ■ Download the CertGenVVD tool and generate the signed certificate for vSphere Replication. See the <i>VMware Validated Design Planning and Preparation</i> documentation.
Email address of Site Recovery Manager administrators	Get the email addresses of the Site Recovery Manager site administrators.

IP Addresses, Host Names, and Network Configuration

In each region, allocate a static IP address and FQDN for Site Recovery Manager, and map the host name to the IP address.

Table 6-1. Network Configuration of Site Recovery Manager in Region A

Setting	Value
Host name	sfo01m01srm01
Static IPv4 address	172.16.11.124
Subnet mask	255.255.255.0
Default gateway	172.16.11.253
DNS server	172.16.11.5,172.16.11.4
FQDN	sfo01m01srm01.sfo01.rainpole.local
Used ports	<ul style="list-style-type: none"> ■ 443 ■ 5678
NTP servers	<ul style="list-style-type: none"> ■ ntp.sfo01.rainpole.local ■ ntp.lax01.rainpole.local

Table 6-2. Network Configuration of Site Recovery Manager in Region B

Setting	Value
Host name	lax01m01srm01
Static IPv4 address	172.17.11.124
Subnet mask	255.255.255.0
Default gateway	172.17.11.253
DNS server	172.17.11.5,172.17.11.4
FQDN	lax01m01srm01.lax01.rainpole.local
Used ports	<ul style="list-style-type: none"> ■ 443 ■ 5678
NTP servers	<ul style="list-style-type: none"> ■ ntp.sfo01.rainpole.local ■ ntp.lax01.rainpole.local

Deploy Site Recovery Manager for VMware Cloud Foundation in Region A

Deploy the new Site Recovery Manager virtual appliance in the protected region.

Procedure

- 1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Setting	Value
URL	https://sfo01m01vc01.sfo01.rainpole.local/ui
User name	administrator@vsphere.local
Password	<i>vsphere_admin_password</i>

- 2 In the **Hosts and clusters** inventory, expand the **sfo01m01vc01.sfo01.rainpole.local** tree and expand the **sfo01-m01dc** data center.
- 3 Deploy the new Site Recovery Manager appliance.
 - a Right-click the **sfo01-m01-mgmt01** cluster and select **Deploy OVF template**.
 - b On the **Select an OVF template** page, select **Local file**, click **Choose files**, use a multiple selection to select the following files from the `bin` folder of the `.iso` mount for Site Recovery Manager Replication, click **Open**, and click **Next**.
 - `srm-va_OVF10.ovf`
 - `srm-va-support.vmdk`
 - `srm-va-system.vmdk`

- c On the **Select a name and folder** page, configure the settings and click **Next**.

Setting	Value
Name	sfo01m01srm01
vCenter Server	sfo01m01vc01.sfo01.rainpole.local
Data center	sfo01-m01dc
Folder	Management VMs

- d On the **Select a compute resource** page, select the **sfo01-m01-mgmt01** cluster and click **Next**.

- e On the **Review details** page, click **Next**.

- f On the **License agreements** page, accept the license agreement and click **Next**.

- g On the **Configuration** page, select the **2 vCPU** configuration and click **Next**.

- h On the **Select storage** page, configure the settings and click **Next**.

Setting	Value
Select virtual disk format	Thin provision
VM Storage Policy	vSAN Default Storage Policy
Datastore	sfo01-m01-vsan01

- i On the **Select networks** page, configure the settings and click **Next**.

Setting	Value
Destination network	sfo01-m01-vds01-management
IP allocation	Static - Manual
IP protocol	IPv4

- j On the **Customize template** page, configure the settings and click **Next**.

Setting	Value
Password	<i>srm_sfo_root_password</i>
Confirm password	<i>srm_sfo_root_password</i>
NTP Servers	ntp.sfo01.rainpole.local,ntp.lax01.rainpole.local
Hostname	sfo01m01srm01.sfo01.rainpole.local
Default Gateway	172.16.11.253
Domain Name	sfo01.rainpole.local
Domain Search Path	sfo01.rainpole.local
Domain Name Servers	172.16.11.5,172.16.11.4
Management Network IP Address	172.16.11.124
Management Network Netmask	255.255.255.0

- k On the **Ready to complete** page, click **Finish**.
- l Right-click the **sfo01m01srm01** virtual machine and select **Power > Power on**.

Replace the Certificate of Site Recovery Manager for VMware Cloud Foundation in Region A

Replace the certificates on Site Recovery Manager in Region A so that Site Recovery Manager can communicate with connected management solutions over a secure connection.

Table 6-3. PKCS#12 Files for Site Recovery Manager in Region A

Site Recovery Manager Instance	Certificate File
sfo01m01srm01.sfo01.rainpole.local	sfo01m01srm01.5.p12

Procedure

- 1 In a Web browser, log in to Site Recovery Manager by using the Virtual Appliance Management Interface (VAMI).

Setting	Value
URL	https://sfo01m01srm01.sfo01.rainpole.local:5480
User name	admin
Password	<i>srm_admin_password</i>

- 2 Upload and install the new certificate.
 - a Click the **Access** tab and in the **Certificate** pane, click **Change**.
 - b On the **Change certificate** page, select the **Use a PKCS #12 certificate file** option and click **Browse**.
 - c Browse to the C:\certs folder, select the **sfo01m01srm01.5.p12** file, and enter the certificate password that you specified when generating the PKCS#12 file and click **Change**.
 - d After you upload the SSL certificate, close the browser.
- 3 Log back in to Site Recovery Manager by using the Virtual Appliance Management Interface.

Setting	Value
User name	admin
Password	<i>srm_sfo_admin_password</i>

- 4 Click the **Access** tab and in the **Certificate** pane, verify that the section shows the updated certificate information.

Configure the Site Recovery Manager Appliance for VMware Cloud Foundation in Region A

To start protecting virtual machines, you must configure the Site Recovery Manager Appliance to connect to a vCenter Server instance on both the protected and the recovery sites.

Procedure

- 1 In a Web browser, log in to Site Recovery Manager by using the Virtual Appliance Management Interface (VAMI).

Setting	Value
URL	https://sfo01m01srm01.sfo01.rainpole.local:5480
User name	admin
Password	<i>srm_admin_password</i>

- 2 Click the **Summary** tab, and click **Configure appliance**.
- 3 On the **Platform Services Controller** page, configure the settings, and click **Next**.

Setting	Value
PSC host name	sfo01m01psc01.sfo01.rainpole.local
PSC port	443
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 4 In the **Security Alert** dialog box, click **Connect**.
- 5 On the **vCenter Server** page, select the **sfo01m01vc01.sfo01.rainpole.local** vCenter Server instance, and click **Next**.
- 6 In the **Security alert** dialog box, click **Connect**.
- 7 On the **Name and extension** page, configure the settings, and click **Next**.

Setting	Value
Site name	sfo01m01srm01.sfo01.rainpole.local
Administrator email	<i>srm_admin_sfo_email_address</i>
Local host	sfo01m01srm01.sfo01.rainpole.local
Extension ID	Default extension ID (com.vmware.vcDr)

- 8 On the **Ready to complete** page, review your settings and click **Finish**.

Deploy Site Recovery Manager for VMware Cloud Foundation in Region B

Deploy the new Site Recovery Manager virtual appliance in the recovery region.

Procedure

- 1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Settings	Value
URL	https://lax01m01vc01.lax01.rainpole.local/ui
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Hosts and clusters** inventory, expand the **lax01m01vc01.lax01.rainpole.local** tree and expand the **lax01-m01dc** data center.
- 3 Deploy the new Site Recovery Manager appliance.
 - a Right-click the **lax01-m01-mgmt01** cluster and select **Deploy OVF template**.
 - b On the **Select an OVF template** page, select **Local file**, click **Choose files**, use a multiple selection to select the following files from the **bin** folder of the **.iso** mount for Site Recovery Manager Replication, click **Open**, and click **Next**.
 - srm-va_OVF10.ovf
 - srm-va-support.vmdk
 - srm-va-system.vmdk
 - c On the **Select a name and folder** page, configure the settings and click **Next**.

Setting	Value
Name	lax01m01srm01
vCenter Server	lax01m01srm01.lax01.rainpole.local
Data center	lax01-m01dc
Folder	Management VMs

- d On the **Select a compute resource** page, select the **lax01-m01-mgmt01** cluster and click **Next**.
- e On the **Review details** page, click **Next**.
- f On the **License agreements** page, accept the license agreement and click **Next**.
- g On the **Configuration** page, select the **2 vCPU** configuration and click **Next**.

- h On the **Select storage** page, configure the settings and click **Next**.

Setting	Value
Select virtual disk format	Thin provision
VM Storage Policy	vSAN Default Storage Policy
Datastore	lax01-m01-vsan01

- i On the **Select networks** page, configure the settings and click **Next**.

Setting	Value
Destination network	lax01-m01-vds01-management
IP allocation	Static - Manual
IP protocol	IPv4

- j On the **Customize template** page, configure the settings and click **Next**.

Setting	Value
Password	<i>srm_lax_root_password</i>
Confirm password	<i>srm_lax_root_password</i>
NTP Servers	ntp.lax01.rainpole.local,ntp.sfo01.rainpole.local
Hostname	lax01m01srm01.lax01.rainpole.local
Default Gateway	172.17.11.253
Domain Name	lax01.rainpole.local
Domain Search Path	lax01.rainpole.local
Domain Name Servers	172.17.11.5,172.17.11.4
Management Network IP Address	172.17.11.124
Management Network Netmask	255.255.255.0

- k On the **Ready to complete** page, click **Finish**.

- l Right-click the **lax01m01srm01** virtual machine and select **Power > Power on**.

Replace the Certificate of Site Recovery Manager for VMware Cloud Foundation in Region B

Replace the certificates on Site Recovery Manager in Region B so that Site Recovery Manager can communicate with connected management solutions over a secure connection.

Table 6-4. PKCS#12 Files for Site Recovery Manager in Region B

Site Recovery Manager Instance	Certificate File
lax01m01srm01.lax01.rainpole.local	lax01m01srm01.5.p12

Procedure

- 1 In a Web browser, log in to Site Recovery Manager by using the Virtual Appliance Management Interface (VAMI).

Setting	Value
URL	https://lax01m01srm01.lax01.rainpole.local:5480
User name	admin
Password	<i>srm_admin_password</i>

- 2 Upload and install the new certificate.
 - a Click the **Access** tab and in the **Certificate** pane, click **Change**.
 - b On the **Change certificate** page, select the **Use a PKCS #12 certificate file** option and click **Browse**.
 - c Browse to the C:\certs folder, select the **lax01m01srm01.5.p12** file, and enter the certificate password that you specified when generating the PKCS#12 file and click **Change**.
 - d After you upload the SSL certificate, close the browser.
- 3 Log back in to Site Recovery Manager by using the Virtual Appliance Management Interface.

Setting	Value
User name	admin
Password	<i>srm_lax_admin_password</i>

- 4 Click the **Access** tab and in the **Certificate** pane, verify that the section shows the updated certificate information.

Configure the Site Recovery Manager Appliance for VMware Cloud Foundation in Region B

To start protecting virtual machines, you must configure the Site Recovery Manager Appliance to connect to a vCenter Server instance on both the protected and the recovery sites.

Procedure

- 1 In a Web browser, log in to Site Recovery Manager by using the Virtual Appliance Management Interface (VAMI).

Setting	Value
URL	https://lax01m01srm01.lax01.rainpole.local:5480
User name	admin
Password	<i>srm_admin_password</i>

- 2 Click the **Summary** tab, and click **Configure appliance**.

3 On the **Platform Services Controller** page, configure the settings, and click **Next**.

Setting	Value
PSC host name	lax01m01psc01.lax01.rainpole.local
PSC port	443
User name	administrator@vsphere.local
Password	vsphere_admin_password

4 In the **Security Alert** dialog box, click **Connect**.

5 On the **vCenter Server** page, select the **lax01m01vc01.lax01.rainpole.local** vCenter Server instance, and click **Next**.

6 In the **Security alert** dialog box, click **Connect**.

7 On the **Name and extension** page, configure the settings, and click **Next**.

Setting	Value
Site name	lax01m01srm01.lax01.rainpole.local
Administrator email	<i>srm_admin_lax_email_address</i>
Local host	lax01m01srm01.lax01.rainpole.local
Extension ID	Default extension ID (com.vmware.vcDr)

8 On the **Ready to complete** page, review your settings and click **Finish**.

Assign Licenses to the Site Recovery Manager Instances for VMware Cloud Foundation

After both Site Recovery Manager Instances are deployed, assign the appropriate licensing.

Procedure

1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Setting	Value
URL	https://sfo01m01vc01.sfo01.rainpole.local/ui
User name	administrator@vsphere.local
Password	<i>vsphere_admin_password</i>

2 Add a new license for the Site Recovery Manager instances.

a In the **Administration** inventory, in the left pane, select **Licensing > Licenses**.

b Click the **Licenses** tab and click **Add new licenses**.

The **New license** wizard opens.

c On the **Enter license keys** page, enter license keys for Site Recovery Manager, and click **Next**.

- d On the **Edit license name** page, enter a descriptive name for the license key, and click **Next**.
 - e On the **Ready to complete** page, review your entries, and click **Finish**.
- 3 Assign the newly added license to the Site Recovery Manager assets.
- a On the **Licenses** page, click the **Assets** tab, and click **Solutions**.
 - b Select the **sfo01m01vc01.sfo01.rainpole.local** instance and click the **Assign License** icon.
 - c Select the license from the list and click **OK**.
 - d Select the **lax01m01vc01.lax01.rainpole.local** instance and click the **Assign License** icon.
 - e Select the license from the list and click **OK**.

Connect the Protected and Recovery Sites for VMware Cloud Foundation

After you deploy Site Recovery Manager in the protected and the recovery regions, connect the instances to configure a site pair.

Procedure

- 1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Setting	Value
URL	https://sfo01m01vc01.sfo01.rainpole.local/ui
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Site Recovery** inventory, on the **sfo01m01vc01.sfo01.rainpole.local** site pane, click **Open Site Recovery**.

The **Site Recovery** page opens.

- 3 Log in to the VMware Site Recovery Manager user interface by using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

Note Authentication is required if the connection between the protected and the recovery sites has been interrupted after the last successful authentication.

- 4 On the **Site Recovery** page, click **New site pair**.

The **New site pair** wizard opens.

5 On the **Site details** page, configure the settings, and click **Next**.

Setting	Value
Select a local vCenter Server	sfo01m01vc01.sfo01.rainpole.local
Second site	Platform Services Controller
PSC host name	lax01m01psc01.lax01.rainpole.local
PSC port	443
User name	administrator@vsphere.local
Password	vsphere_admin_password

6 In the **Security alert** dialog box, click **Connect**

7 On the **vCenter Server and services** page, select **lax01m01vc01.lax01.rainpole.local** vCenter Server and select **Site Recovery Manager (com.vmware.vcDr)** service and click **Next**.

8 In the **Security alert** dialog box, click **Connect** .

9 On the **Ready to complete** page, review your settings and click **Finish**.

Configure Mappings between the Protected and the Recovery Regions for VMware Cloud Foundation

Configure resource mappings between the protected and the recovery sites to enable failover of vRealize Suite Lifecycle Manager, vRealize Operations Manager, and vRealize Automation.

Procedure

1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Setting	Value
URL	https://sfo01m01vc01.sfo01.rainpole.local/ui
User name	administrator@vsphere.local
Password	vsphere_admin_password

2 In the **Site Recovery** inventory, on the **sfo01m01vc01.sfo01.rainpole.local** site pane, click **Open Site Recovery**.

The **Site Recovery** page opens.

3 Log in to the VMware Site Recovery Manager user interface by using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

Note Authentication is required if the connection between the protected and the recovery sites has been interrupted after the last successful authentication.

4 On the **sfo01m01vc01.sfo01.rainpole.local** to **lax01m01vc01.lax01.rainpole.local** site pair pane, click **View details**.

5 Configure network mappings.

- a On the main navigation bar, click the **Site pair** tab.
- b In the left pane, click **Network mappings** and click **New**.
The **New network mappings** wizard opens.
- c On the **Creation mode** page, select **Prepare mappings manually** and click **Next**.
- d On the **Recovery networks** page, expand the object trees, select the distributed port groups to map, click **Add mappings**, and click **Next**.

Setting	Value for Protected Region	Value for Recovery Region
vCenter Server	sfo01m01vc01.sfo01.rainpole.local	lax01m01vc01.lax01.rainpole.local
Data center	sfo01-m01dc	lax01-m01dc
Distributed Switch	sfo01-m01-vds01	lax01-m01-vds01
Port group mapping	<i>port_group_prefix-xRegion01-VXLAN</i>	<i>port_group_prefix-xRegion01-VXLAN</i>

- e On the **Reverse mappings** page, select the previously configured mappings and click **Next**.
- f On the **Test networks** page, keep the default values and click **Next**.
- g On the **Ready to complete** page, review your settings and click **Finish**.

6 Configure folder mappings.

- a On the main navigation bar, click the **Site pair** tab.
- b In the left pane, click **Folder mappings** and click **New**.
The **New folder mappings** wizard opens.
- c On the **Creation mode** page, select **Prepare mappings manually** and click **Next**.

- d On the **Recovery folders** page, expand the object trees, select the folders of vRealize Operations Manager, vRealize Suite Lifecycle Manager, and vRealize Automation components, click **Add mappings**, and click **Next**.

Setting	Value for Protected Region	Value for Recovery Region
vCenter Server	sfo01m01vc01.sfo01.rainpole.local	lax01m01vc01.lax01.rainpole.local
Data center	sfo01-m01dc	lax01-m01dc
vRealize Operations Manager folder mapping	sfo01-m01fd-vrops	lax01-m01fd-vrops
vRealize Suite Lifecycle Manager folder mapping	sfo01-m01fd-mgmt	lax01-m01fd-mgmt
vRealize Automation folder mapping	sfo01-m01fd-vra	lax01-m01fd-vra

- e On the **Reverse mappings** page, select the previously configured mappings and click **Next**.
- f On the **Ready to complete** page, review your settings and click **Finish**.

7 Configure resource mappings.

- a On the main navigation bar, click the **Site pair** tab.
- b In the left pane, click **Resource mappings** and click **New**.

The **New resource mappings** wizard opens.

- c On the **Recovery resources** page, select the clusters for Region A and Region B to create a mapping between the resource in the clusters, click **Add mappings**, and click **Next**.

Setting	Value for Protected Region	Value for Recovery Region
vCenter Server	sfo01m01vc01.sfo01.rainpole.local	lax01m01vc01.lax01.rainpole.local
Data center	sfo01-m01dc	lax01-m01dc
Cluster mapping	sfo01-m01-mgmt01	lax01-m01-mgmt01

- d On the **Reverse mappings** page, select the previously configured mappings and click **Next**.
- e On the **Ready to complete** page, review your settings and click **Finish**.

8 Configure a placeholder datastore.

- a On the main navigation bar, click the **Site pair** tab.
- b In the left pane, click **Placeholder datastores**, select the **sfo01m01vc01.sfo01.rainpole.local** site, and click **New**.
- c In the **New placeholder datastore** dialog box, select the **sfo01-m01-vsan01** datastore and click **Add**.
- d On the **Placeholder datastores** page, select the **lax01m01vc01.lax01.rainpole.local** site, and click **New**.
- e In the **New placeholder datastore** dialog box, select the **lax01-m01-vsan01** datastore and click **Add**.

Configure Operations Management for the Business Continuity Components for VMware Cloud Foundation

7

After you install Site Recovery Manager in Region A and Region B, enable its integration with the operations management layer. You can monitor and receive alerts and logs about site protection and disaster recovery in a central location by using vRealize Operations Manager and vRealize Log Insight.

Procedure

- 1 [Connect vRealize Operations Manager to Site Recover Manager for VMware Cloud Foundation](#)
Install and configure the vRealize Operations Management Pack for Site Recovery Manager to monitor the health and configuration of the Site Recovery Manager instances, and the status of the protection groups and recovery plans for failing over the management components of the SDDC.
- 2 [Connect vRealize Log Insight to Site Recovery Manager for VMware Cloud Foundation](#)
To monitor and troubleshoot the operation of the Site Recovery Manager appliance in the region by using vRealize Log Insight, install and configure the vRealize Log Insight agent on the appliance.

Connect vRealize Operations Manager to Site Recover Manager for VMware Cloud Foundation

Install and configure the vRealize Operations Management Pack for Site Recovery Manager to monitor the health and configuration of the Site Recovery Manager instances, and the status of the protection groups and recovery plans for failing over the management components of the SDDC.

Procedure

- 1 [Install the vRealize Operations Manager Management Pack for Site Recovery Manager for VMware Cloud Foundation](#)
Install the .pak file for the management pack for Site Recovery Manager to add the management pack as a solution to vRealize Operations Manager.
- 2 [Add SRM Adapter Instances to vRealize Operations Manager for VMware Cloud Foundation](#)
In a dual-region SDDC, configure SRM Adapters to collect monitoring data in vRealize Operations Manager about the Site Recovery Manager instances and failover objects.

Install the vRealize Operations Manager Management Pack for Site Recovery Manager for VMware Cloud Foundation

Install the .pak file for the management pack for Site Recovery Manager to add the management pack as a solution to vRealize Operations Manager.

Procedure

- 1 In a Web browser, log in to vRealize Operations Manager by using the operations interface.

Setting	Value
URL	https://vrops01svr01.rainpole.local
User name	admin
Password	<i>vrops_admin_password</i>

- 2 On the main navigation bar, click **Administration**.
- 3 In the left pane, navigate to **Solutions > Repository**.
- 4 Click **Add a management pack**.
The **Add solution** dialog box opens.
- 5 On the **Select solution** page, click **Browse**, navigate to the vRealize Operations Management Pack for Site Recovery Manager .pak file, click **Open**, and click **Upload**.
- 6 After the upload is complete, click **Next**.
- 7 On the **End user license agreement** page, accept the license agreement and click **Next**.
- 8 On the **Install** page, after the installation is complete, click **Finish**. on the **Install** page.

Add SRM Adapter Instances to vRealize Operations Manager for VMware Cloud Foundation

In a dual-region SDDC, configure SRM Adapters to collect monitoring data in vRealize Operations Manager about the Site Recovery Manager instances and failover objects.

Procedure

- 1 In a Web browser, log in to vRealize Operations Manager by using the operations interface.

Setting	Value
URL	https://vrops01svr01.rainpole.local
User name	admin
Password	<i>vrops_admin_password</i>

- 2 On the main navigation bar, click **Administration**.
- 3 In the left pane, navigate to **Solutions > Configuration**.

- 4 In the **Solutions** section, select **SRM adapter**, and under **Configured adapter instances**, click the **Configure** icon.

The **Manage solution - SRM Adapter** dialog box opens.

- 5 In the **Instance name** section, click the Add icon and, in the **Instance settings** section, configure the settings for the Site Recovery Manager instances.

Setting	Value for Site Recovery Manager in Region A	Value for Site Recovery Manager in Region B
Display Name	SRM Adapter - sfo01m01srm01	SRM Adapter - lax01m01srm01
Description	Site Recovery Manager Adapter for sfo01	Site Recovery Manager Adapter for lax01
SRM Host	sfo01m01srm01.sfo01.rainpole.local	lax01m01srm01.lax01.rainpole.local
SRM Port	443	443
Credential name	SRM Adapter Credentials - sfo01m01srm01	SRM Adapter Credentials - lax01m01srm01
User name	administrator@vsphere.local	administrator@vsphere.local
Password	<i>vsphere_admin_password</i>	<i>vsphere_admin_password</i>

- 6 Click **Test Connection** to validate the connection to Site Recovery Manager.
- 7 Click **Save Settings**.
- 8 Repeat the steps to configure the Site Recovery Manager adapter for the Region B instance.
- 9 In the **Manage Solution - SRM adapter** dialog box, click **Close**.

Results

The SRM Adapter instances appear on the **Solutions** page of the vRealize Operations Manager user interface. The **Collection state** of the adapter is **Collecting** and the **Collection status** is **Data receiving**.

Connect vRealize Log Insight to Site Recovery Manager for VMware Cloud Foundation

To monitor and troubleshoot the operation of the Site Recovery Manager appliance in the region by using vRealize Log Insight, install and configure the vRealize Log Insight agent on the appliance.

Procedure

- 1 [Install the vRealize Log Insight Agent on Site Recovery Manager](#)

To start sending log data from the Site Recovery Manager appliance to vRealize Log Insight, first install the vRealize Log Insight agent for Linux on the appliance in each region.

2 Configure the vRealize Log Insight Agent on the Site Recovery Manager

After you install the vRealize Log Insight agent on the Site Recovery Manager appliance, to start forwarding log events to vRealize Log Insight, configure the agent with the location of the vRealize Log Insight cluster, set the log ingestion API as the protocol for remote logging, and disable SSL-enabled log collection.

Install the vRealize Log Insight Agent on Site Recovery Manager

To start sending log data from the Site Recovery Manager appliance to vRealize Log Insight, first install the vRealize Log Insight agent for Linux on the appliance in each region.

You repeat this procedure twice to install the vRealize Log Insight agent on the Site Recovery Manager instances for the protected and the recovery region.

Setting	Value for the Protected Region	Value for the Recovery Region
Site Recovery Manager instance	sfo01m01srm01.sfo01.rainpole.local	lax01m01srm01.lax01.rainpole.local
vRealize Log Insight instance	sfo01vrli01.sfo01.rainpole.local	lax01vrli01.lax01.rainpole.local
VIP address of the integrated load balancer of vRealize Log Insight	192.168.31.10	192.168.32.10

Procedure

- 1 In a Web browser, log in to vRealize Log Insight by using the user interface.

Setting	Value
URL	https://sfo01vrli01.sfo01.rainpole.local
User name	admin
Password	<i>vrli_admin_password</i>

- 2 Click the configuration drop-down menu icon and select **Administration**.
- 3 Under **Management**, click **Agents**.
- 4 On the **Agents** page, click the **Download Log Insight Agent** link.
- 5 In the **Download Log Insight Agent** dialog box, click **Linux RPM (32-bit/64-bit)** and save the .rpm file.

6 Enable SSH access in the Site Recovery Manager appliance.

- a In a Web browser, log in to Site Recovery Manager by using the Virtual Appliance Management Interface (VAMI).

Setting	Value
URL	https://sfo01m01srm01.sfo01.rainpole.local:5480
User name	admin
Password	<i>srm_admin_password</i>

- b On the **SRM Appliance Management** page, select **Access** and click **Enable** from the **SSH** pane.

7 By using an scp client such as WinSCP, copy the VMware-Log-Insight-Agent-4.8.0-xxxxxx.noarch.192.168.31.10.rpm file to the /tmp folder on the Site Recovery Manager appliance.

8 Log in to the Site Recovery Manager appliance by using a Secure Shell (SSH) client.

Setting	Value
FQDN	sfo01m01srm01.sfo01.rainpole.local
User name	admin
Password	<i>srm_admin_password</i>

9 Install the vRealize Log Insight Linux agent by running the command.

```
sudo rpm -i /tmp/VMware-Log-Insight-Agent-4.8.0-xxxxxx.noarch.192.168.31.10.rpm
```

10 Configure the vRealize Log Insight agent to start automatically.

```
sudo systemctl enable liagentd
```

11 Repeat this procedure for the lax01m01srm01.lax01.rainpole.local Site Recovery Manager instance in Region B.

Configure the vRealize Log Insight Agent on the Site Recovery Manager

After you install the vRealize Log Insight agent on the Site Recovery Manager appliance, to start forwarding log events to vRealize Log Insight, configure the agent with the location of the vRealize Log Insight cluster, set the log ingestion API as the protocol for remote logging, and disable SSL-enabled log collection.

Procedure

- 1 Log in to the Site Recovery Manager appliance by using a Secure Shell (SSH) client.

Setting	Value
FQDN	sfo01m01srm01.sfo01.rainpole.local
User name	admin
Password	<i>srm_admin_password</i>

- 2 Open the `liagent.ini` file for editing by using a text editor such as `vi`.

```
sudo vi /var/lib/loginsight-agent/liagent.ini
```

- 3 Locate the `[server]` section, remove the comment for these parameters, insert the following values, and save the file.

```
[server]
hostname=sfo01vrli01.sfo01.rainpole.local

; Hostname or IP address of your Log Insight server / cluster load balancer. Default:
;hostname=LOGINSIGHT

; Protocol can be cfapi (Log Insight REST API), syslog, syslog_udp. Default:
proto=cfapi

; Log Insight server port to connect to. Default ports for protocols:
; syslog and syslog_udp: 514; syslog with ssl: 6514; cfapi: 9000; cfapi with ssl: 9543. Default:
port=9000

; SSL usage. Default:
ssl=no
; Example of configuration with trusted CA:
;ssl=yes
;ssl_ca_path=/etc/pki/tls/certs/ca.pem

; Time in minutes to force reconnection to the server.
; This option mitigates imbalances caused by long-lived TCP connections. Default:
;reconnect=30
```

- 4 Restart the vRealize Log Insight agent on the appliance.

```
sudo systemctl restart liagentd
```

- 5 Verify that the vRealize Log Insight agent is running on the appliance.

```
sudo systemctl status liagentd
```

6 Repeat this procedure for the Site Recovery Manager in region B using the following settings.

Setting	Value
Site Recovery Manager	lax01m01srm01.lax01.rainpole.local
Log Insight	lax01vri01.lax01.rainpole.local

Failover of the SDDC Management Applications for VMware Cloud Foundation

8

Configure and perform a failover of the management applications in the SDDC from the protected region, Region A, to the recovery region, Region B. Failing over these applications maintains the operational state of the SDDC.

You fail over the following management applications:

- vRealize Suite Lifecycle Manager
- Analytics cluster of vRealize Operations Manager
- Primary components of vRealize Automation with embedded vRealize Orchestrator.

The vSphere Proxy Agents of vRealize Automation is not failed over. Deploy a separate pair of agents in region B in an application isolated network.

Table 8-1. Support for Failover of the SDDC Management Applications

Management Component	Supports Failover
vRealize Suite Lifecycle Manager	Yes
vRealize Operations Manager analytics nodes	Yes
vSphere proxy agents	No
vRealize Automation appliance	Yes
Microsoft SQL server	Yes
IaaS Components	Yes

Procedure

1 [Complete the Configuration for Failover of the SDDC Management Applications for VMware Cloud Foundation](#)

Prepare the management applications in the SDDC for failover or planned migration. Replicate application-specific VMs by using vSphere Replication and create recovery plans for them by using Site Recovery Manager. To fully recreate the SDDC configuration of Region A in Region B if failover occurs, configure vSphere DRS rules for high availability of the management virtual machines.

2 [Test Failover of the SDDC Management Applications for VMware Cloud Foundation](#)

You can identify potential problems during a future failover by testing the recovery plan for the management applications in the SDDC.

3 [Perform Planned Migration of the SDDC Management Applications for VMware Cloud Foundation](#)

After you have successfully configured and tested failover of the management applications, you can initiate a migration process from Region A to Region B. The planned migration of the SDDC management components keeps the SDDC operational, for example, when upgrading the hardware or changing the network configuration in Region A.

4 [Perform Disaster Recovery of the SDDC Management Applications for VMware Cloud Foundation](#)

Prepare networking in Region B and perform a failover of vRealize Automation, vRealize Operations Manager, and vRealize Suite Lifecycle Manager to Region B if Region A becomes unavailable.

Complete the Configuration for Failover of the SDDC Management Applications for VMware Cloud Foundation

Prepare the management applications in the SDDC for failover or planned migration. Replicate application-specific VMs by using vSphere Replication and create recovery plans for them by using Site Recovery Manager. To fully recreate the SDDC configuration of Region A in Region B if failover occurs, configure vSphere DRS rules for high availability of the management virtual machines.

- [Configure Replication, Create Protection Group and Recovery Plan for the Operations Management Applications for VMware Cloud Foundation](#)

Configure the replication of the virtual machines that participate in the analytics cluster of the vRealize Operations Manager and vRealize Lifecycle Manager to support failover to Region B. Replica virtual machines become active upon failover. You create a protection group and recovery plan along with the replication.

- [Customize the Recovery Plan for the Operations Management Applications for VMware Cloud Foundation](#)

After you create the recovery plan, configure the startup priority and the startup and shutdown options for the virtual machines of the analytics cluster and vRealize Suite Lifecycle Manager. The master node of vRealize Operations Manager must start first after failover.

- [Configure Replication, Create Protection Group and Recovery Plan for the Cloud Management Applications for VMware Cloud Foundation](#)

To support failover to Region B, enable the replication of the virtual machines that constitute the primary functionality of the Cloud Management Platform. Replica virtual machines become active upon failover. You create a protection group and recovery plan along with the replication.

- [Customize the Recovery Plan for the Cloud Management Platform for VMware Cloud Foundation](#)

After you create the recovery plan for the Cloud Management Platform VMs, configure the startup priority, and the startup and shutdown options for the virtual machines.

- [Create an Anti-Affinity Rule for vRealize Operations Manager for VMware Cloud Foundation in Region B](#)

Anti-affinity rules do not persist across regions during recovery using Site Recovery Manager. You must create the anti-affinity rules for the analytics virtual machines in Region B so that the rules still apply after a failover of vRealize Operations Manager.

- [Create Anti-Affinity Rules for vRealize Automation for VMware Cloud Foundation in Region B](#)

Anti-affinity rules do not persist across regions during recovery using Site Recovery Manager. In Region B, you must create the anti-affinity rules for the components of the Cloud Management Platform that are failed over from Region A so that the rules apply after failover.

- [Create Virtual Machine Groups to Define the Startup Order of the Cloud Management Platform for VMware Cloud Foundation in Region B](#)

You can use virtual machine groups to define the startup order of virtual machines. vSphere HA follows this order when powering on the virtual machines in the group. In Region B, create the virtual machine groups defining the startup order of the cloud management virtual machines that are failed over from Region A.

Configure Replication, Create Protection Group and Recovery Plan for the Operations Management Applications for VMware Cloud Foundation

Configure the replication of the virtual machines that participate in the analytics cluster of the vRealize Operations Manager and vRealize Lifecycle Manager to support failover to Region B. Replica virtual machines become active upon failover. You create a protection group and recovery plan along with the replication.

Procedure

- 1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Setting	Value
URL	https://sfo01m01vc01.sfo01.rainpole.local/ui
User name	administrator@vsphere.local
Password	<i>vsphere_admin_password</i>

- 2 In the **Site Recovery** inventory, on the **sfo01m01vc01.sfo01.rainpole.local** site pane, click **Open Site Recovery**.

The **Site Recovery** page opens.

- 3 Log in to the VMware Site Recovery Manager user interface by using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	<i>vsphere_admin_password</i>

Note Authentication is required if the connection between the protected and the recovery sites has been interrupted after the last successful authentication.

- 4 On the **sfo01m01vc01.sfo01.rainpole.local** to **lax01m01vc01.lax01.rainpole.local** site pair pane, click **View details**.

- 5 On the main navigation bar, click the **Replications** tab and, in the left pane, select **Outgoing**.
- 6 On the **sfo01m01vc01.sfo01.rainpole.local** to **lax01m01vc01.lax01.rainpole.local** pair, click **New**.
The **Configure replication** wizard opens.
- 7 In the **sfo01m01vc01.sfo01.rainpole.local - lax01m01vc01.lax01.rainpole.local** pair, click **New**.
The **Configure replication** wizard opens.
- 8 On the **Virtual machines** page, select the following virtual machines and click **Next**.

Virtual Machine Name	Role
vrops01svr01a	Master node
vrops01svr01b	Master replica node
vrops01svr01c	Data node 1
vrslcm01svr01	Realize Suite Lifecycle Manager

- 9 On the **Target site** page, select **Auto-assign vSphere Replication server** and click **Next**.
- 10 On the **Target datastore** page, configure the settings and click **Next**.

Setting	Value
Disk format	Thin provision
VM storage policy	vSAN Default Storage Policy
Datastore	lax01-m01-vsan01

- 11 On the **Replication settings** page, enter the following settings and click **Next**.

Setting	Value
Recovery Point Objective (RPO)	15 minutes
Enable point in time instances	Selected Keep 3 instances per day for the last 1 days.
Enable Guest OS quiescing	Deselected
Enable network compression for VR data	Selected

Important Do not enable guest OS quiescing because some of the vRealize Operations Manager databases do not support quiescing. Quiescing might result in a cluster failure because virtual disks remain in a frozen state for too long.

Compression requires extra resources. Do not enable it if the hosts are over-utilized.

- 12 On the **Protection group** page, select **Add to new protection group**, enter **SDDC Operations Management PG** for the protection group name, and click **Next**.
- 13 On the **Recovery plan** page, select **Add to new recovery plan**, enter **SDDC Operations Management RP** for recovery plan name, and click **Next**.

- 14 On the **Ready to complete** page, review the configuration and click **Finish**.

Customize the Recovery Plan for the Operations Management Applications for VMware Cloud Foundation

After you create the recovery plan, configure the startup priority and the startup and shutdown options for the virtual machines of the analytics cluster and vRealize Suite Lifecycle Manager. The master node of vRealize Operations Manager must start first after failover.

Procedure

- 1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Setting	Value
URL	https://sfo01m01vc01.sfo01.rainpole.local/ui
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Site Recovery** inventory, on the **sfo01m01vc01.sfo01.rainpole.local** site pane, click **Open Site Recovery**.

The **Site Recovery** page opens.

- 3 Log in to the VMware Site Recovery Manager user interface by using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

Note Authentication is required if the connection between the protected and the recovery sites has been interrupted after the last successful authentication.

- 4 On the **sfo01m01vc01.sfo01.rainpole.local** to **lax01m01vc01.lax01.rainpole.local** site pair pane, click **View details**.
- 5 On the main navigation bar, click the **Recovery plans** tab and, in the left pane, navigate to **Recovery plans > SDDC Operations Management RP**.
- 6 On the **SDDC Operations Management RP** page, click the **Recovery steps** tab.
- 7 Change the startup priority of the virtual machine of the master node.
- In the **Recovery step** section, expand **Power on priority 3 VMs**.
 - Right-click **vrops01svr01a** and select **Priority group > 1 (Highest)**.
 - In the **Change priority** dialog box, confirm the change.

- 8 Configure startup and shutdown options for the vRealize Operations Manager master node.
 - a In the **Recovery step** section, expand **Power on priority 1 VMs**.
 - b Right-click vrops01svr01a and select **Configure recovery**.
 - c In the **Recovery properties** page, expand the **Shutdown action** section and set the **Shutdown guest OS before power off** timeout to **10 minutes**.
 - d Expand the **Startup action** section, set the **Wait for VMware tools** timeout to **10 minutes**, and click **OK**.
- 9 Repeat the steps to configure startup priority and startup and shutdown options for the remaining virtual machines.

Virtual Machine	Power on Priority Order	Shutdown Timeout	Startup Timeout
vrops01svr01b	2	-	-
vrops01svr01c	3	10 minutes	10 minutes
vrslcm01svr01	4	-	-

Configure Replication, Create Protection Group and Recovery Plan for the Cloud Management Applications for VMware Cloud Foundation

To support failover to Region B, enable the replication of the virtual machines that constitute the primary functionality of the Cloud Management Platform. Replica virtual machines become active upon failover. You create a protection group and recovery plan along with the replication.

Procedure

- 1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Setting	Value
URL	https://sfo01m01vc01.sfo01.rainpole.local/ui
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Site Recovery** inventory, on the **sfo01m01vc01.sfo01.rainpole.local** site pane, click **Open Site Recovery**.

The **Site Recovery** page opens.

3 Log in to the VMware Site Recovery Manager user interface by using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

Note Authentication is required if the connection between the protected and the recovery sites has been interrupted after the last successful authentication.

- 4 On the **sfo01m01vc01.sfo01.rainpole.local** to **lax01m01vc01.lax01.rainpole.local** site pair pane, click **View details**.
- 5 On the main navigation bar, click the **Replications** tab and, in the left pane, select **Outgoing**.
- 6 On the **sfo01m01vc01.sfo01.rainpole.local** to **lax01m01vc01.lax01.rainpole.local** pair, click **New**. The **Configure replication** wizard opens.
- 7 On the **Virtual machines** page, select the following virtual machines and click **Next**.

Virtual Machine Name	Role
vra01ims01a	IaaS Manager Service and DEM Orchestrator
vra01ims01b	IaaS Manager Service and DEM Orchestrator
vra01iws01a	IaaS Web Server
vra01iws01b	IaaS Web Server
vra01mssql01	Microsoft SQL Server
vra01svr01a	vRealize Automation Appliance
vra01svr01b	vRealize Automation Appliance
vra01svr01c	vRealize Automation Appliance
vra01dem01a	vRealize Automation DEM Worker
vra01dem01b	vRealize Automation DEM Worker

- 8 On the **Target site** page, select **Auto-assign vSphere Replication server** and click **Next**.
- 9 On the **Target datastore** page, configure the settings and click **Next**.

Setting	Value
Disk format	Thin provision
VM storage policy	vSAN Default Storage Policy
Datastore	lax01-m01-vsant01

10 On the **Replication settings** page, enter the following settings and click **Next**.

Setting	Value
Recovery Point Objective (RPO)	15 minutes
Enable point in time instances	Selected
	Keep 3 instances per day for the last 1 days.
Enable Guest OS quiescing	Deselected
Enable network compression for VR data	Selected

Important Do not enable guest OS quiescing because some of the vRealize Operations Manager databases do not support quiescing. Quiescing might result in a cluster failure because virtual disks remain in a frozen state for too long.

Compression requires extra resources. Do not enable it if the hosts are over-utilized.

- 11 On the **Protection group** page, select **Add to new protection group**, enter **SDDC CCloud Management PG** for the protection group name, and click **Next**.
- 12 On the **Recovery plan** page, select **Add to new recovery plan**, enter **SDDC CCloud Management RP** for recovery plan name, and click **Next**.
- 13 On the **Ready to complete** page, review the configuration and click **Finish**.

Customize the Recovery Plan for the Cloud Management Platform for VMware Cloud Foundation

After you create the recovery plan for the Cloud Management Platform VMs, configure the startup priority, and the startup and shutdown options for the virtual machines.

You configure the power on priority, dependencies, and additional startup delay for the virtual machines in the Cloud Management Platform.

Table 8-2. Recovery Steps Configuration of the Cloud Management Platform

VM Name	Power on Priority	Dependency	Additional Startup Delay
vra01mssql01	1	-	-
vra01svr01a	1	-	5
vra01svr01b	2	vra01svr01a	-
vra01svr01c	2	vra01svr01b	-
vra01iws01a	3	-	5
vra01iws01b	3	vra01iws01a	5
vra01ims01a	4	-	5
vra01ims01b	4	vra01ims01a	5
vra01dem01a	5	-	-
vra01dem01b	5	-	-

Procedure

- 1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Setting	Value
URL	https://sfo01m01vc01.sfo01.rainpole.local/ui
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Site Recovery** inventory, on the **sfo01m01vc01.sfo01.rainpole.local** site pane, click **Open Site Recovery**.

The **Site Recovery** page opens.

- 3 Log in to the VMware Site Recovery Manager user interface by using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

Note Authentication is required if the connection between the protected and the recovery sites has been interrupted after the last successful authentication.

- 4 On the main navigation bar, click the **Recovery plans** tab, and, in the left pane, navigate to **Recovery plans > SDDC Cloud Management RP**.
- 5 On the **SDDC Operations Management RP** page, click the **Recovery steps** tab.
- 6 Change the startup priority of the vra01mssql01 virtual machine.
 - a In the **Recovery step** section, expand **Power on priority 3 VMs**.
 - b Right-click **vra01mssql01** and select **Priority group > 1 (Highest)**.
 - c In the **Change priority** dialog box, confirm the change.
- 7 Repeat the step to reconfigure the power on priority of the remaining virtual machines.

- 8 Insert a break point (User prompt) in the recovery plan for the vRealize Automation cluster.
 - a In the **Recovery step** section, right-click **Power on priority 2 VMs**, select **Add step before**, configure the settings, and click **Add**.

Setting	Value
Type	Prompt
Name	User Prompt
Content	Refer to KB article 74879 and take necessary action.

- b Repeat the step to insert a break point (user prompt) in the recovery plan before priority 3 VMs.

Note The vRealize Automation cluster has nodes in two priority virtual machine groups, you add the prompt before **Power on priority 2 VMs** and **Power on priority 3 VMs**.

- 9 Configure dependencies between the virtual machines that have the vRA Server role.
 - a On the **Recovery steps** tab, expand **Power on priority 2 VMs**, right-click the **vra01svr01b**, and select **Configure recovery**.
The **VM recovery properties** dialog box opens.
 - b On the **Recovery properties** tab, expand the **VM Dependencies** section, and, from the **View VM dependencies** drop-down button, select **View all**.
 - c Select **vra01svr01a** and click **OK**.
- 10 Repeat the step to configure dependencies for the remaining virtual machines.
- 11 Configure additional startup delay for the primary vRA Server.
 - a On the **Recovery steps** tab, expand **Power on priority 1 VMs**, right-click the **vra01svr01a**, and select **Configure recovery**.
The **VM recovery properties** dialog box opens.
 - b On the **Recovery properties** tab, expand the **Startup action** section, select **Additional delay**, set the delay time to **5 minutes**, and click **OK**.
 - c Click **OK**.
- 12 Repeat this step to configure additional startup delay for the remaining virtual machines.

Create an Anti-Affinity Rule for vRealize Operations Manager for VMware Cloud Foundation in Region B

Anti-affinity rules do not persist across regions during recovery using Site Recovery Manager. You must create the anti-affinity rules for the analytics virtual machines in Region B so that the rules still apply after a failover of vRealize Operations Manager.

Procedure

- 1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Settings	Value
URL	https://lax01m01vc01.lax01.rainpole.local/ui
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Hosts and clusters** inventory, expand the **lax01m01vc01.lax01.rainpole.local** tree and expand the **lax01-m01dc** data center.
- 3 Select the **lax01-m01-mgmt01** cluster and click the **Configure** tab.
- 4 In the left pane, navigate to **Configuration > VM/Host rules** and click **Add**.
The **Create VM/Host rule** dialog box opens.
- 5 Configure the settings and click **OK**.

Setting	Value
Name	anti-affinity-rule-vropsm
Enable rule	Selected
Type	Separate Virtual Machines
Members	<ul style="list-style-type: none"> ■ vrops01svr01a.rainpole.local ■ vrops01svr01b.rainpole.local ■ vrops01svr01c.rainpole.local

Create Anti-Affinity Rules for vRealize Automation for VMware Cloud Foundation in Region B

Anti-affinity rules do not persist across regions during recovery using Site Recovery Manager. In Region B, you must create the anti-affinity rules for the components of the Cloud Management Platform that are failed over from Region A so that the rules apply after failover.

You configure the following anti-affinity rules for the vRealize Automation virtual machines.

Table 8-3. Anti-Affinity Rules for the Cloud Management Platform

Name	Type	Members
anti-affinity-rule-vra-svr	Separate Virtual Machines	<ul style="list-style-type: none"> ■ vra01svr01a ■ vra01svr01b ■ vra01svr01c
anti-affinity-rule-vra-dem	Separate Virtual Machines	<ul style="list-style-type: none"> ■ vra01dem01a ■ vra01dem01b

Table 8-3. Anti-Affinity Rules for the Cloud Management Platform (continued)

Name	Type	Members
anti-affinity-rule-vra-ims	Separate Virtual Machines	<ul style="list-style-type: none"> ■ vra01ims01a ■ vra01ims01b
anti-affinity-rule-vra-iws	Separate Virtual Machines	<ul style="list-style-type: none"> ■ vra01iws01a ■ vra01iws01b

Procedure

- 1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Settings	Value
URL	https://lax01m01vc01.lax01.rainpole.local/ui
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Hosts and clusters** inventory, expand the **lax01m01vc01.lax01.rainpole.local** tree and expand the **lax01-m01dc** data center.
- 3 Select the **lax01-m01-mgmt01** cluster and click the **Configure** tab.
- 4 In the left pane, navigate to **Configuration > VM/Host rules** and click **Add**.
The **Create VM/Host rule** dialog box opens.
- 5 Configure the settings and click **OK**.

Setting	Value
Name	anti-affinity-rule-vra-svr
Enable rule	Selected
Type	Separate Virtual Machines
Members	<ul style="list-style-type: none"> ■ vra01svr01a ■ vra01svr01b ■ vra01svr01c

- 6 Repeat the procedure to configure the remaining anti-affinity rules.

Create Virtual Machine Groups to Define the Startup Order of the Cloud Management Platform for VMware Cloud Foundation in Region B

You can use virtual machine groups to define the startup order of virtual machines. vSphere HA follows this order when powering on the virtual machines in the group. In Region B, create the virtual machine groups defining the startup order of the cloud management virtual machines that are failed over from Region A.

You configure VM/Host groups and rules for the vRealize Automation virtual machines.

Table 8-4. VM-Host Group Configuration for Failover of the SDDC Management Applications

VM-Host Group Name	VM-Host Group Member
vRealize Automation IaaS Database	vra01mssql01
vRealize Automation Virtual Appliances	vra01svr01a
	vra01svr01b
	vra01svr01c
vRealize Automation IaaS Web Servers	vra01iws01a
	vra01iws01b
vRealize Automation IaaS Managers	vra01ims01a
	vra01ims01b
vRealize Automation IaaS DEM Workers	vra01dem01a
	vra01dem01b
vRealize Automation IaaS Proxy Agents	lax01ias01a
	lax01ias01b

Table 8-5. VM-Host Rule Configuration for the Restart Order of the Cloud Management Applications After Failover

VM/Host Rule Name	First Restart Virtual Machines in Group	Then Restart Virtual Machines in Group
SDDC Cloud Management Platform 01	vRealize Automation IaaS Database	vRealize Automation Virtual Appliances
SDDC Cloud Management Platform 02	vRealize Automation Virtual Appliances	vRealize Automation IaaS Web Servers
SDDC Cloud Management Platform 03	vRealize Automation IaaS Web Servers	vRealize Automation IaaS Managers
SDDC Cloud Management Platform 04	vRealize Automation IaaS Managers	vRealize Automation IaaS DEM Workers
SDDC Cloud Management Platform 05	vRealize Automation IaaS Managers	vRealize Automation IaaS Proxy Agents

Procedure

- 1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Settings	Value
URL	https://lax01m01vc01.lax01.rainpole.local/ui
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Hosts and clusters** inventory, expand the **lax01m01vc01.lax01.rainpole.local** tree and expand the **lax01-m01dc** data center.
- 3 Select the **lax01-m01-mgmt01** cluster and click the **Configure** tab.

- 4 Create a virtual machine group for the Microsoft SQL Server instance.
 - a In the left pane, navigate to **Configuration > VM/Host groups** and click **Add**.
The **Create VM/Host group** dialog box opens.
 - b Configure the settings and click **OK**.

Setting	Value
	vRealize Automation IaaS Database
Type	VM Group
Members	vra01mssql01

- 5 Repeat to this step to create the remaining VM/Host groups.
- 6 Create a VM/Host rule to power on the vRealize Automation database before the vRealize Automation virtual appliances.
 - a In the left pane, navigate to **Configuration > VM/Host rules** and click **Add**.
The **Create VM/Host rule** dialog box opens.
- 7 Configure the settings and click **OK**.

Setting	Value
Name	SDDC Cloud Management Platform 01
Enable rule	Selected
Type	Virtual Machines to Virtual Machines
The VM dependency restart condition must be met before continuing to	vRealize Automation IaaS Database
On restart for VM group	vRealize Automation Virtual Appliances

- 8 Repeat to this step to create the remaining VM/Host rules.

Test Failover of the SDDC Management Applications for VMware Cloud Foundation

You can identify potential problems during a future failover by testing the recovery plan for the management applications in the SDDC.

- [Test Failover of the Operations Management Applications for VMware Cloud Foundation](#)
Validate the configuration for failover of vRealize Operations Manager and vRealize Suite Lifecycle Manager by testing the recovery plan for the operations management applications in advance.
- [Test Failover of the Cloud Management Platform for VMware Cloud Foundation](#)
Validate the configuration for failover of vRealize Automation by testing the recovery plan for the cloud management applications in advance.

Test Failover of the Operations Management Applications for VMware Cloud Foundation

Validate the configuration for failover of vRealize Operations Manager and vRealize Suite Lifecycle Manager by testing the recovery plan for the operations management applications in advance.

Site Recovery Manager runs the analytics nodes of vRealize Operations Manager and vRealize Suite Lifecycle Manager on the test network and on a temporary snapshot of replicated data in Region B.

Procedure

- 1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Setting	Value
URL	https://sfo01m01vc01.sfo01.rainpole.local/ui
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Site Recovery** inventory, on the **sfo01m01vc01.sfo01.rainpole.local** site pane, click **Open Site Recovery**.

The **Site Recovery** page opens.

- 3 Log in to the VMware Site Recovery Manager user interface by using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

Note Authentication is required if the connection between the protected and the recovery sites has been interrupted after the last successful authentication.

- 4 On the **sfo01m01vc01.sfo01.rainpole.local** to **lax01m01vc01.lax01.rainpole.local** site pair pane, click **View details**.
- 5 On the main navigation bar, click the **Recovery plans** tab and, in the left pane, navigate to **Recovery plans > SDDC Operations Management RP**.
- 6 Click the **Recovery steps** tab, and click the **Test** button.
The **Test - SDDC Operations Management RP** dialog box opens.
- 7 On the **Confirmation options** page, leave the **Replicate recent changes to recovery site** check box selected and click **Next**.
- 8 On the **Ready to complete** page, click **Finish** to initiate the test recovery.
- 9 After the test recovery process finishes, to clean up all the created test virtual machines, click the **Cleanup** button.

The **Cleanup - SDDC Operations Management RP** dialog box opens.

10 On the **Confirmation options** page, click **Next**.

11 On the **Ready to complete** page, click **Finish**.

After the clean-up process finishes, **Plan status** must be Ready.

Test Failover of the Cloud Management Platform for VMware Cloud Foundation

Validate the configuration for failover of vRealize Automation by testing the recovery plan for the cloud management applications in advance.

Site Recovery Manager runs the vRealize Automation virtual machines on the test network and on a temporary snapshot of replicated data in Region B.

Procedure

1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Setting	Value
URL	https://sfo01m01vc01.sfo01.rainpole.local/ui
User name	administrator@vsphere.local
Password	<i>vsphere_admin_password</i>

2 In the **Site Recovery** inventory, on the **sfo01m01vc01.sfo01.rainpole.local** site pane, click **Open Site Recovery**.

The **Site Recovery** page opens.

3 Log in to the VMware Site Recovery Manager user interface by using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	<i>vsphere_admin_password</i>

Note Authentication is required if the connection between the protected and the recovery sites has been interrupted after the last successful authentication.

4 On the **sfo01m01vc01.sfo01.rainpole.local** to **lax01m01vc01.lax01.rainpole.local** site pair pane, click **View details**.

5 On the main navigation bar, click the **Recovery plans** tab and, in the left pane, navigate to **Recovery plans > SDDC Cloud Management RP**.

6 Click the **Recovery steps** tab, and click the **Test** button.

The **Test - SDDC Operations Management RP** dialog box opens.

7 On the **Confirmation options** page, leave the **Replicate recent changes to recovery site** check box selected and click **Next**.

- 8 On the **Ready to complete** page, click **Finish** to initiate the test recovery.

Note Because recovered virtual machines are using the test network, VMware Tools on the vra01svr01a, vra01svr01b, and vra01svr01c virtual machines might not start within the default timeout. In the recovery plan, increase the startup delay for VMware Tools for these virtual machines to complete the test.

- 9 To resume the recovery plan test, on the **User prompt** dialog box, click **Dismiss**.
- 10 After the test recovery process finishes, to clean up all the created test virtual machines, click the **Cleanup** button.

The **Cleanup - SDDC Operations Management RP** dialog box opens.

- 11 On the **Confirmation options** page, click **Next**.
- 12 On the **Ready to complete** page, click **Finish**.

After the clean-up process finishes, **Plan status** must be Ready.

Perform Planned Migration of the SDDC Management Applications for VMware Cloud Foundation

After you have successfully configured and tested failover of the management applications, you can initiate a migration process from Region A to Region B. The planned migration of the SDDC management components keeps the SDDC operational, for example, when upgrading the hardware or changing the network configuration in Region A.

- [Initiate a Planned Migration of the Operations Management Applications for VMware Cloud Foundation](#)
To migrate the virtual machines of the analytics cluster of vRealize Operations Manager and vRealize Suite Lifecycle Manager from Region A to Region B under planned circumstances, run the recovery plan for the operations management applications.
- [Initiate a Planned Migration of the Cloud Management Platform for VMware Cloud Foundation](#)
To migrate the virtual machines of vRealize Automation from Region A to Region B under planned circumstances, run the recovery plan for the cloud management applications.

Initiate a Planned Migration of the Operations Management Applications for VMware Cloud Foundation

To migrate the virtual machines of the analytics cluster of vRealize Operations Manager and vRealize Suite Lifecycle Manager from Region A to Region B under planned circumstances, run the recovery plan for the operations management applications.

Before failing over the analytics cluster of vRealize Operations Manager, you must take it offline. After the failover operation finishes, you bring the analytics cluster online in Region B.

Procedure

- 1 In a Web browser, log in to the vRealize Operations Manager by using the administration interface.

Settings	Value
URL	https://vrops01svr01a.rainpole.local/admin
User name	admin
Password	<i>vrops_admin_password</i>

- 2 Take the vRealize Operations Manager analytics cluster offline.
 - a In the left pane, click **System status**.
 - b On the **System status** page, under **Cluster status**, click **Take offline**.
 - c In the **Take cluster offline** dialog box, in the **Reason** text box, enter **Planned Migration of the Operations Management applications**, and click **OK**.

Wait until all vRealize Operations Manager nodes are offline and the **Cluster status** becomes Offline.

- 3 In a Web browser, log in to vCenter Server by using the vSphere Client.

Setting	Value
URL	https://sfo01m01vc01.sfo01.rainpole.local/ui
User name	administrator@vsphere.local
Password	<i>vsphere_admin_password</i>

- 4 In the **Site Recovery** inventory, on the **sfo01m01vc01.sfo01.rainpole.local** site pane, click **Open Site Recovery**.

The **Site Recovery** page opens.

- 5 Log in to the VMware Site Recovery Manager user interface by using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	<i>vsphere_admin_password</i>

Note Authentication is required if the connection between the protected and the recovery sites has been interrupted after the last successful authentication.

- 6 On the **sfo01m01vc01.sfo01.rainpole.local** to **lax01m01vc01.lax01.rainpole.local** site pair pane, click **View details**.
- 7 On the main navigation bar, click the **Recovery plans** tab and, in the left pane, navigate to **Recovery plans > SDDC Operations Management RP**.

- 8 To initiate the planned migration of vRealize Operations Manager and vRealize Suite Lifecycle Manager, click the **Recovery steps** tab and click **Run**.

The **Recovery - SDDC Operations Management RP** wizard opens.

- 9 On the **Confirmation options** page, configure the settings for planned migration and click **Next**.

Setting	Value
I understand that this process will permanently alter the virtual machines and infrastructure of both the protected and recovery datacenters.	Selected
Recovery type	Planned migration

- 10 On the **Ready to complete** page, click **Finish**.

- 11 In a Web browser, log in to the vRealize Operations Manager by using the administration interface.

Settings	Value
URL	https://vroops01svr01a.rainpole.local/admin
User name	admin
Password	<i>vroops_admin_password</i>

- 12 Take the vRealize Operations Manager analytics cluster online.

- a In the navigation pane, click **System status**.
- b On the **System status** page, under **Cluster status**, click **Bring online**.

What to do next

- 1 Verify that after failover both vRealize Operations Manager and vRealize Suite Lifecycle Manager are operational. See *Verification of vRealize Operations Manager* and *Verification of vRealize Suite Lifecycle Manager* in the *VMware Validated Design Operational Verification* documentation. If vRealize Operations Manager is not operational, log in to the vRealize Operations Manager master node, take the cluster offline and then bring the cluster back online.
- 2 Prepare vRealize Operations Manager and vRealize Suite Lifecycle Manager for failback by reprotecting the virtual machines of the analytics cluster and vRealize Suite Lifecycle Manager in Site Recovery Manager. See [Reprotect the Operations Management Applications for VMware Cloud Foundation](#).

Initiate a Planned Migration of the Cloud Management Platform for VMware Cloud Foundation

To migrate the virtual machines of vRealize Automation from Region A to Region B under planned circumstances, run the recovery plan for the cloud management applications.

Procedure

- 1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Setting	Value
URL	https://sfo01m01vc01.sfo01.rainpole.local/ui
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Site Recovery** inventory, on the **sfo01m01vc01.sfo01.rainpole.local** site pane, click **Open Site Recovery**.

The **Site Recovery** page opens.

- 3 Log in to the VMware Site Recovery Manager user interface by using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

Note Authentication is required if the connection between the protected and the recovery sites has been interrupted after the last successful authentication.

- 4 On the **sfo01m01vc01.sfo01.rainpole.local** to **lax01m01vc01.lax01.rainpole.local** site pair pane, click **View details**.
- 5 On the main navigation bar, click the **Recovery plans** tab and, in the left pane, navigate to **Recovery plans > SDDC Cloud Management RP**.
- 6 To initiate the planned migration of the Cloud Management Platform, click the **Recovery steps** tab and click **Run**.

The **Recovery - SDDC Cloud Management RP** wizard opens.

- 7 On the **Confirmation options** page, configure the settings for planned migration and click **Next**.

Setting	Value
I understand that this process will permanently alter the virtual machines and infrastructure of both the protected and recovery datacenters.	Selected
Recovery type	Planned migration

- 8 On the **Ready to complete** page, click **Finish**.
- 9 During planned migration, execution of the recovery plan pauses after powering on priority 1 virtual machines and priority 2 virtual machines. Perform the steps in KB article [74879](#) and, on the **User prompt** dialog box, click **Dismiss** to resume the planned migration.

What to do next

- 1 Verify that vRealize Automation virtual machines are operational. See *Operational Verification of the Cloud Management Layer* in the *VMware Validated Design Operational Verification* documentation. If vRealize Automation is not operational, restart the vRealize Automation virtual machines. See *SDDC Startup and Shutdown* in the *VMware Validated Design Operational Verification* documentation.
- 2 Prepare vRealize Automation for failback by reprotecting their virtual machines in Site Recovery Manager. See [Reprotect the Cloud Management Platform for VMware Cloud Foundation](#).

Perform Disaster Recovery of the SDDC Management Applications for VMware Cloud Foundation

Prepare networking in Region B and perform a failover of vRealize Automation, vRealize Operations Manager, and vRealize Suite Lifecycle Manager to Region B if Region A becomes unavailable.

After failover of the Operations Management and Cloud Management components, SDDC manager in Region A cannot manage the vRealize products. All relevant SDDC Manager workflows related to the vRealize products are available again after Region A is restored and the necessary post failback operations are performed.

Procedure

- 1 [Assign the Primary Role to the NSX Manager Instance for the Management Cluster for VMware Cloud Foundation in Region B](#)

If Region A becomes unavailable, you must prepare the network layer in Region B for a failover of the management applications. First change the role of the NSX Manager instance in Region B to primary to recreate the virtual network infrastructure in Region B.

- 2 [Deploy the Control VM of the Universal Distributed Logical Router for VMware Cloud Foundation in Region B](#)

After the SDDC deployment, the universal NSX components for dynamic routing are placed in Region A. If a site failure occurs in Region A, the SDDC management applications might lose connectivity if you fail them over to Region B. Deploy and configure a control VM for the universal distributed logical router sfo01m01udlr01 in Region B to provide dynamic routing to the SDDC management applications.

- 3 [Reconfigure the Universal Distributed Logical Router and NSX Edge Nodes for Dynamic Routing for VMware Cloud Foundation in Region B](#)

To support dynamic routing in Region B before you initiate disaster recovery from Region A, configure the universal distributed logical router sfo01m01udlr01 and NSX Edge nodes lax01m01esg01 and lax01m01esg02. This configuration ensures that the management components of the SDDC continue to communicate using optimal routes in a fault-tolerant network.

4 [Verify Establishment of BGP for the Universal Distributed Logical Router for VMware Cloud Foundation in Region B](#)

Verify that the universal distributed logical router for the management applications is successfully peering, and that BGP routing has been established in Region B. After you perform disaster recovery, they can continue communicating to keep the SDDC operational.

5 [Deploy the NSX Controllers for the NSX Instance for VMware Cloud Foundation in Region B](#)

Deploy the three-node universal NSX Controller cluster in Region B for logical switching and routing in and across the clusters and regions in the SDDC.

6 [Connect the Application NSX Load Balancer in Region B to the SDDC Network for VMware Cloud Foundation](#)

Enable the network connectivity on lax01m01lb01 load balancer to support high availability and distribute the network traffic load for vRealize Operations Manager, vRealize Suite Lifecycle Manager, and the Cloud Management Platform after disaster recovery to Region B.

7 [Initiate Disaster Recovery of the Operations Management Applications for VMware Cloud Foundation in Region B](#)

If a site failure in Region A occurs, initiate disaster recovery of vRealize Suite Lifecycle Manager and of vRealize Operations Manager to keep the monitoring functionality of the SDDC running.

8 [Initiate Disaster Recovery of the Cloud Management Platform for VMware Cloud Foundation in Region B](#)

If a site failure in Region A occurs, initiate disaster recovery of the vRealize Automation components to keep the workload provisioning functionality of the SDDC available.

9 [Post-Failover Configuration of the SDDC Management Applications for VMware Cloud Foundation](#)

After failover of the Cloud Management Platform, vRealize Operations Manager, and vRealize Suite Lifecycle Manager, you must perform additional tasks to ensure that the management applications work as expected.

10 [Additional Post-Failover Configuration After Region A Is Available Again for VMware Cloud Foundation](#)

When the original protected region, Region A, is back online, you can fully transfer all features of the SDDC configuration to Region B. Integrate the running management nodes in Region A in the main SDDC configuration that is failed over to Region B.

Assign the Primary Role to the NSX Manager Instance for the Management Cluster for VMware Cloud Foundation in Region B

If Region A becomes unavailable, you must prepare the network layer in Region B for a failover of the management applications. First change the role of the NSX Manager instance in Region B to primary to recreate the virtual network infrastructure in Region B.

You first disconnect the NSX Manager for the management cluster in Region B from the primary NSX Manager in Region A that is offline.

Procedure

- 1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Settings	Value
URL	https://lax01m01vc01.lax01.rainpole.local/ui
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Networking and security** inventory, click **Installation and upgrade**.
- 3 On the **Management** tab, click the **NSX Managers** tab.
- 4 Disconnect the NSX Manager instance for the management cluster in Region B from the primary NSX Manager instance in Region A.
 - a Select the IP address of the NSX Manager instance for Region B **172.17.11.65**.
 - b From the **Actions** menu, select **Disconnect from primary NSX Manager**.
 - c In the **Disconnect from Primary NSX Manager** dialog box, click **Yes**.
The operation sets the role of the NSX Manager instance to transit.
- 5 Promote the NSX Manager for the management cluster in Region B to the primary role.
 - a From the **Actions** menu, select **Assign primary role**.
 - b In the **Assign primary role** dialog box, click **Yes**.

Deploy the Control VM of the Universal Distributed Logical Router for VMware Cloud Foundation in Region B

After the SDDC deployment, the universal NSX components for dynamic routing are placed in Region A. If a site failure occurs in Region A, the SDDC management applications might lose connectivity if you fail them over to Region B. Deploy and configure a control VM for the universal distributed logical router sfo01m01udlr01 in Region B to provide dynamic routing to the SDDC management applications.

Procedure

- 1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Settings	Value
URL	https://lax01m01vc01.lax01.rainpole.local/ui
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Networking and security** inventory, click **NSX Edges**.
- 3 From the **NSX Manager** drop-down menu, select **172.17.11.65**.

- 4 Redeploy the control VMs of the universal distributed logical router.
 - a Click **sfo01m01udlr01**.
 - b Click the **Configure** tab and, in the left pane, click **Appliance settings**.
 - c In the **Edge appliance VMs** section, click the **Add** icon in the edge appliance card.
 - d In the **Add Edge appliance VM** dialog box, configure the settings and click **Add**.

Setting	Value
Data center	lax01-m01dc
Cluster/Resource Pool	lax01-m01-mgmt01
Datastore	lax01-m01-vsan01

- e Repeat this step to deploy a second NSX Edge appliance with the same configuration.
- 5 Configure high availability for the control VMs of the universal distributed logical router.
 - a On the **Configure** tab for sfo01m01udlr01, in the left pane, click **High availability**.
 - b In the **Management/HA interface** section, click **Edit**, set **Connected to** to **lax01-m01-vds01-management** and click **Save**.
 - c In the **High availability configuration** section, click **Edit**, configure the settings and click **Save**.

Setting	Value
HA Status	Enable
Declare Dead Time	15
Logging	Enable
Log Level	Info

- 6 Configure the credentials for running commands on the control VMs of the universal logical router.
 - a From the **Actions** menu at the top of the **sfo01m01udlr01** page, select **Change CLI credentials**.
 - b In the **Change CLI credentials** dialog box, configure the settings and click **OK**.

Setting	Value
User Name	admin
Password	<i>udlr_admin_password</i>
Confirm Password	<i>udlr_admin_password</i>

Reconfigure the Universal Distributed Logical Router and NSX Edge Nodes for Dynamic Routing for VMware Cloud Foundation in Region B

To support dynamic routing in Region B before you initiate disaster recovery from Region A, configure the universal distributed logical router sfo01m01udlr01 and NSX Edge nodes lax01m01esg01

and lax01m01esg02. This configuration ensures that the management components of the SDDC continue to communicate using optimal routes in a fault-tolerant network.

Procedure

- 1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Settings	Value
URL	https://lax01m01vc01.lax01.rainpole.local/ui
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Networking and security** inventory, click **NSX Edges**.
- 3 From the **NSX Manager** drop-down menu, select **172.17.11.65**.
- 4 Verify the routing configuration for the universal distributed logical router.
 - a Click **sfo01m01udlr01**.
 - b Click the **Routing** tab and verify the settings.

Setting	Value
Global Configuration > Routing Configuration > ECMP	Started
Global Configuration > Dynamic Routing Configuration > Router ID	192.168.10.3

- 5 To verify the protocol settings and configure BGP peering between the UDLR device and the NSX Edge nodes for the ECMP-enabled North-South routing in Region B, on the left side, select **BGP**.
 - a Verify the settings.

Setting	Value
Status	Started
Local AS	65003
Graceful Restart	Stopped

- b Under **Neighbors**, select **192.168.10.50** and click the **Edit** icon.

The **192.168.10.50** entry represents the connection settings for the lax01m01esg01 neighbor

- c In the **Edit BGP Neighbor** dialog box, change the **Weight** value to **60**, enter the BGP password that was configured during the initial setup of the UDLR, and click **Save**.

Setting	Value for lax01m01esg01	Value for lax01m01esg02
IP Address	192.168.10.50	192.168.10.51
Forwarding Address	192.168.10.3	192.168.10.3
Protocol Address	192.168.10.4	192.168.10.4
Remote AS	65003	65003
Weight	60	60
Keep Alive Time	1	1
Hold Down Time	3	3
Password	<i>BGP_password</i>	<i>BGP_password</i>

- d On the **BGP** page, repeat the steps for the **192.168.10.51** neighbor which represents the lax01m01esg02 device.
- e Click **Publish**.

- 6 On the left side, select **Route Redistribution** to verify redistribution status.

Category	Setting	Value
Route Redistribution Status	OSPF	Deselected
	BGP	Enabled
Route Redistribution table	Learner	BGP
	From	Connected
	Prefix	Any
	Action	Permit

- 7 Reconfigure the routing and weight values of lax01m01esg01 and lax01m01esg02 edges.
- a Return to the NSX Edges page with the **172.17.11.65** option selected in the **NSX Manager** drop-down menu.
 - b Click the edge link of **lax01m01esg01** to open its configuration interface.
 - c Click the **Routing** tab.
 - d On the left side, select **BGP**, select the **192.168.10.4** neighbor, and click the **Edit** icon.
 - e In the **Edit Neighbor** dialog box, change the **Weight** value to **60** and click **OK**.
 - f Click **Publish**.
 - g Repeat the steps for the lax01m01esg02 edge.

Verify Establishment of BGP for the Universal Distributed Logical Router for VMware Cloud Foundation in Region B

Verify that the universal distributed logical router for the management applications is successfully peering, and that BGP routing has been established in Region B. After you perform disaster recovery, they can continue communicating to keep the SDDC operational.

Procedure

- 1 Log in to the Universal Distributed Logical Router by using a Secure Shell (SSH) client.

Setting	Value
FQDN	sfo01m01udlr01
User name	admin
Password	<i>udlr_admin_password</i>

- 2 Verify that the UDLR can peer with the ECMP-enabled NSX Edge services gateways.
 - a To display information about the BGP and TCP connections to the UDLR neighbors, run the `show ip bgp neighbors` command.
 - b In the command output, verify that the BGP state is `Established`, up for 192.168.10.50 (`lax01m01esg01`) and 192.168.10.51 (`lax01m01esg02`).
- 3 Verify that the UDLR receives routes by using BGP and that multiple routes are established to BGP-learned networks.
 - a Run the `show ip route` command.
 - b In the command output, verify that the routes to the networks are marked with the letter B and several routes to each adjacent network exist.

The letter B in front of each route indicates that this route is established over BGP.

Deploy the NSX Controllers for the NSX Instance for VMware Cloud Foundation in Region B

Deploy the three-node universal NSX Controller cluster in Region B for logical switching and routing in and across the clusters and regions in the SDDC.

Procedure

- 1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Settings	Value
URL	<code>https://lax01m01vc01.lax01.rainpole.local/ui</code>
User name	<code>administrator@vsphere.local</code>
Password	<i>vsphere_admin_password</i>

2 Deploy the universal controller cluster in Region B.

You deploy three NSX Controller nodes with the same configuration.

- a In the **Networking and security** inventory, click **Installation and upgrade**.
- b On the **Management** tab, click the **NSX Controller nodes** tab.
- c From the **NSX Manager** drop-down menu, select **172.17.11.65**.
- d Under **Controller nodes**, click the **Add** icon.
- e If you deploy the first NSX Controller node, in the **Add Controller** dialog box, configure the settings and click **Next**.

Setting	Value
Password	<i>mgmtnsx_controllers_password</i>
Confirm Password	<i>mgmtnsx_controllers_password</i>

- f In the **Deployment & connectivity** dialog box, configure the settings and click **Finish**.

Setting	Value
Name	<ul style="list-style-type: none"> ■ lax01m01nsrc01 for the first NSX Controller ■ lax01m01nsrc02 for the second NSX Controller ■ lax01m01nsrc03 for the third NSX Controller
Data center	<i>lax01-m01dc</i>
Cluster/Resource Pool	<i>lax01-m01-mgmt01</i>
Datastore	<i>lax01-m01-vsan01</i>
Folder	<i>lax01-m01fd-nsx</i>
Connected To	<i>lax01-m01-vds01-management</i>
Select IP Pool	<i>lax01-mgmt01-nsrc01</i>

- g After the **Status** of the controller node that you are deploying changes to Connected, repeat the step to deploy the remaining two NSX Controller nodes *lax01m01nsrc02* and *lax01m01nsrc03*.

3 Synchronize the state of the newly deployed controllers by using the Update Controller State mechanism on the NSX Manager instance in Region B.

An Update Controller State operation pushes the current VXLAN and universal distributed logical router configuration from NSX Manager to the NSX Controller cluster.

- a In the **Networking and security** inventory, click **Installation and Upgrade**.
- b On the **Management** tab, click the **NSX Managers** tab and select the **172.17.11.65** instance.
- c From the **Actions** drop-down menu, select **Update Controller ctate**.
- d In the **Update Controller ctate** dialog box, click **Yes**.

- 4 Configure the DRS anti-affinity VM/Host rule for the newly deployed NSX Controller nodes.
 - a In the **Hosts and clusters** inventory, expand the **lax01m01vc01.lax01.rainpole.local** tree and expand the **lax01-m01dc** data center.
 - b Select the **lax01-m01-mgmt01** cluster.
 - c Click the **Configure** tab and under **Configuration**, select **VM/Host rules**.
 - d To create an anti-affinity rule, in the **VM/Host rules** list, click **Add**.
 - e In the **Create VM/Host rule** dialog box, configure the settings and click **OK**.

Setting	Value
Name	anti-affinity-rule-nsxc
Enable rule	Selected
Type	Separate Virtual Machines
Members	<ul style="list-style-type: none"> ■ lax01m01nsxc01 ■ lax01m01nsxc02 ■ lax01m01nsxc03

Connect the Application NSX Load Balancer in Region B to the SDDC Network for VMware Cloud Foundation

Enable the network connectivity on lax01m01lb01 load balancer to support high availability and distribute the network traffic load for vRealize Operations Manager, vRealize Suite Lifecycle Manager, and the Cloud Management Platform after disaster recovery to Region B.

Procedure

- 1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Settings	Value
URL	https://lax01m01vc01.lax01.rainpole.local/ui
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Networking and security** inventory, click **NSX Edges**.
- 3 From the **NSX Manager** drop-down menu, select **172.17.11.65**.
- 4 Click the edge link of the **lax01m01lb01** device.
- 5 Click the **Configure** tab.
- 6 Click **Interfaces**, select the **mgmt-vnic-vrealize-edge** vNIC, and click **Edit**.
- 7 In the **Edit interface** dialog box, set **Connectivity status** to **Connected** and click **Save**.

Initiate Disaster Recovery of the Operations Management Applications for VMware Cloud Foundation in Region B

If a site failure in Region A occurs, initiate disaster recovery of vRealize Suite Lifecycle Manager and of vRealize Operations Manager to keep the monitoring functionality of the SDDC running.

Procedure

- 1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Settings	Value
URL	https://lax01m01vc01.lax01.rainpole.local/ui
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Site Recovery** inventory, on the **lax01m01vc01.lax01.rainpole.local** site pane, click **Open Site Recovery**.

The **Site Recovery** page opens.

- 3 Log in to the VMware Site Recovery Manager user interface by using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

Note Authentication is required if the connection between the protected and the recovery sites has been interrupted after the last successful authentication.

- 4 On the **lax01m01vc01.lax01.rainpole.local** to **sfo01m01vc01.sfo01.rainpole.local** site pair pane, click **View details**.
- 5 On the main navigation bar, click the **Recovery plans** tab and, in the left pane, navigate to **Recovery plans > SDDC Operations Management RP**.
- 6 To initiate the failover of vRealize Operations Manager and vRealize Suite Lifecycle Manager, click the **Recovery steps** tab and click **Run**.

The **Recovery - SDDC Operations Management RP** wizard opens.

- 7 On the **Confirmation options** page, configure the settings for disaster recovery and click **Next**.

Setting	Value
I understand that this process will permanently alter the virtual machines and infrastructure of both the protected and recovery datacenters.	Selected
Recovery type	Disaster recovery

- 8 On the **Ready to complete** page, click **Finish**.

What to do next

- 1 Verify that vRealize Suite Lifecycle Manager is up and operates correctly after a failover. See *Verification of vRealize Suite Lifecycle Manager* in the *VMware Validated Design Operational Verification* documentation.
- 2 Verify that vRealize Operations Manager is up and operates correctly after a failover. See *Verification of vRealize Operations Manager* in the *VMware Validated Design Operational Verification* documentation. If vRealize Operations Manager is not operational, log in to the vRealize Operations Manager master node, take the cluster offline and then bring the cluster back online.
- 3 Complete the SDDC configuration in Region B. See [Post-Failover Configuration of the SDDC Management Applications for VMware Cloud Foundation](#).
- 4 Prepare vRealize Operations Manager and vRealize Suite Lifecycle Manager for failback by reprotecting the virtual machines of the analytics cluster and the vRealize Suite Lifecycle Manager in Site Recovery Manager. See [Reprotect the Operations Management Applications for VMware Cloud Foundation](#).

Initiate Disaster Recovery of the Cloud Management Platform for VMware Cloud Foundation in Region B

If a site failure in Region A occurs, initiate disaster recovery of the vRealize Automation components to keep the workload provisioning functionality of the SDDC available.

Procedure

- 1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Settings	Value
URL	https://lax01m01vc01.lax01.rainpole.local/ui
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Site Recovery** inventory, on the **lax01m01vc01.lax01.rainpole.local** site pane, click **Open Site Recovery**.

The **Site Recovery** page opens.

- 3 Log in to the VMware Site Recovery Manager user interface by using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

Note Authentication is required if the connection between the protected and the recovery sites has been interrupted after the last successful authentication.

- 4 On the **lax01m01vc01.lax01.rainpole.local** to **sfo01m01vc01.sfo01.rainpole.local** site pair pane, click **View details**.
- 5 On the main navigation bar, click the **Recovery plans** tab and, in the left pane, navigate to **Recovery plans > SDDC Cloud Management RP**.
- 6 To initiate the failover of the Cloud Management Platform, click the **Recovery steps** tab and click **Run**.

The **Recovery - SDDC Cloud Management RP** wizard opens.

- 7 On the **Confirmation options** page, configure the settings for planned migration and click **Next**.

Setting	Value
I understand that this process will permanently alter the virtual machines and infrastructure of both the protected and recovery datacenters.	Selected
Recovery type	Disaster recovery

- 8 On the **Ready to complete** page, click **Finish**.
- 9 During disaster recovery, execution of the recovery plan pauses after powering on priority 1 virtual machines and priority 2 virtual machines. Perform the steps in KB article [74879](#) and, on the **User prompt** dialog box, click **Dismiss** to resume the planned migration.

What to do next

- 1 Verify that vRealize Automation virtual machines are operational. See *Operational Verification of the Cloud Management Layer* in the *VMware Validated Design Operational Verification* documentation. If vRealize Automation is not operational, restart the vRealize Automation virtual machines. See *SDDC Startup and Shutdown* in the *VMware Validated Design Operational Verification* documentation.
- 2 Complete the SDDC configuration in Region B. See [Post-Failover Configuration of the SDDC Management Applications for VMware Cloud Foundation](#).
- 3 Prepare vRealize Automation for failback by reprotecting their virtual machines in Site Recovery Manager. See [Reprotect the Cloud Management Platform for VMware Cloud Foundation](#).

Post-Failover Configuration of the SDDC Management Applications for VMware Cloud Foundation

After failover of the Cloud Management Platform, vRealize Operations Manager, and vRealize Suite Lifecycle Manager, you must perform additional tasks to ensure that the management applications work as expected.

Procedure

- 1 [Configure the UDLR Control Virtual Machine to Forward Events to vRealize Log Insight for VMware Cloud Foundation in Region B](#)

Configure the UDLR control VM instances for the management cluster to forward log information to vRealize Log Insight in Region B.

2 Update the DNS Record for vRealize Log Insight for VMware Cloud Foundation in Region A

After you fail over the management applications in the SDDC to Region B, to send logs to the vRealize Log Insight instance in Region B, you update the DNS record for vRealize Log Insight in the to point to the Region B instance.

3 Connect vRealize Operations Manager to vRealize Log Insight for VMware Cloud Foundation in Region B

After disaster recovery to Region B, vRealize Operations Manager is still connected to the vRealize Log Insight instance in Region A. Because of the site failure in Region A, the vRealize Log Insight instance in Region A is not accessible. Configure the vRealize Log Insight Adapter to integrate vRealize Operations Manager with vRealize Log Insight in Region B.

Configure the UDLR Control Virtual Machine to Forward Events to vRealize Log Insight for VMware Cloud Foundation in Region B

Configure the UDLR control VM instances for the management cluster to forward log information to vRealize Log Insight in Region B.

Procedure

- 1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Settings	Value
URL	https://lax01m01vc01.lax01.rainpole.local/ui
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Networking and security** inventory, click **NSX Edges**.
- 3 Configure the newly deployed control VM of the UDLR in Region B to forward events to vRealize Log Insight in Region B.
 - a From the **NSX Manager** drop-down menu, select **172.17.11.65**.
 - b Click the edge link of the **sfo01m01udlr01** device.
 - c Click the **Configure** tab and, in the left pane, click **Appliance settings**.
 - d Click the **Configuration** icon and select **Change syslog configuration**.
 - e In the **Change Syslog Servers** dialog box, configure the settings and click **OK**.

Setting	Value
Server 1	192.168.32.10
Protocol	UDP

Update the DNS Record for vRealize Log Insight for VMware Cloud Foundation in Region A

After you fail over the management applications in the SDDC to Region B, to send logs to the vRealize Log Insight instance in Region B, you update the DNS record for vRealize Log Insight in the to point to the Region B instance.

You modify the DNS record for `sfo01vrli01.sfo01.rainpole.local` to point to the IP address `192.168.32.10` of `lax01vrli01.lax01.rainpole.local` in Region B.

Procedure

- 1 Log in to the DNS server `dc51rp1.rainpole.local` that resides in Region B as an Active Directory administrator by using a Remote Desktop Protocol (RDP) connection.
- 2 Open the Windows **Start** menu, enter `dns` in the **Search** text box, and press Enter.
The **DNS Manager** dialog box appears.
- 3 In the **DNS Manager** dialog box, under **Forward Lookup Zones**, select the `sfo01.rainpole.local` domain by expanding the tree and locate the `sfo01vrli01` record on the right side.
- 4 Double-click the `sfo01vrli01` record, change the IP address of the record from `192.168.31.10` to **`192.168.32.10`** and click **OK**.

Setting	Value
Fully qualified domain name (FQDN)	<code>sfo01vrli01.sfo01.rainpole.local</code>
IP Address	<code>192.168.32.10</code>
Update associated pointer (PTR) record	Selected

Connect vRealize Operations Manager to vRealize Log Insight for VMware Cloud Foundation in Region B

After disaster recovery to Region B, vRealize Operations Manager is still connected to the vRealize Log Insight instance in Region A. Because of the site failure in Region A, the vRealize Log Insight instance in Region A is not accessible. Configure the vRealize Log Insight Adapter to integrate vRealize Operations Manager with vRealize Log Insight in Region B.

Procedure

- 1 In a Web browser, log in to the vRealize Operations Manager by using the operations interface.

Settings	Value
URL	<code>https://vrops01svr01.rainpole.local</code>
User name	<code>admin</code>
Password	<code>vrops_admin_password</code>

- 2 On the main navigation bar, click **Administration**.
- 3 In the left pane, navigate to **Solutions > Configuration**.

- 4 In the **Solutions** section, select **VMware vRealize Log Insight**, and, in the **Configured adapter instances** section, click **Configure**.

The **Manage solution - VMware vRealize Log Insight** dialog box opens.

- 5 In the **Instance settings** pane, modify the settings for the connection to vRealize Log Insight.

Setting	Value
Display Name	Log Insight Adapter - lax01vrli01
Description	vRealize Log Insight for lax01
Log Insight server	lax01vrli01.lax01.rainpole.local

- 6 To verify that vRealize Operations Manager can connect to vRealize Log Insight, click **Test connection** and in the **Info** dialog box click **OK**.
- 7 Click **Save settings** and in the **Info** dialog box click **OK**.
- 8 In the **Manage solution - VMware vRealize Log Insight** dialog box, click **Close**.

Results

The vRealize Log Insight Adapter is available on the **Solutions** page of the vRealize Operations Manager user interface. The **Collection State** of the adapter is **Collecting** and the **Collection Status** is **Data receiving**.

Additional Post-Failover Configuration After Region A Is Available Again for VMware Cloud Foundation

When the original protected region, Region A, is back online, you can fully transfer all features of the SDDC configuration to Region B. Integrate the running management nodes in Region A in the main SDDC configuration that is failed over to Region B.

Procedure

- 1 [Reconfigure the NSX Instance for the Management Cluster for VMware Cloud Foundation in Region A](#)

When Region A is back online after a disaster recovery to Region B, to avoid conflicts in the management and control planes of NSX, modify the roles of the NSX Managers and delete certain NSX components in Region A.

- 2 [Disconnect the Application NSX Load Balancer from the SDDC Network for VMware Cloud Foundation in Region A](#)

Because operations management and cloud management applications are failed over to Region B, disconnect the NSX load balancer for the SDDC management applications in Region A. If the load balancer remains connected to the network, the load balancer might receive data for a management application that is failed over to the other region.

3 [Configure Routing Between Region A and Region B After Failover for VMware Cloud Foundation](#)

When Region A is back online after a disaster recovery to Region B, you must update the routing configuration to restore routing between Region B and Region A and to optimize route selection.

4 [Restore the Original DNS Record for vRealize Log Insight for VMware Cloud Foundation in Region A](#)

When Region A is back online, update the DNS record for the vRealize Log Insight instance in Region A with the original IP address so that the management applications that are running again in Region A can start sending log data to vRealize Log Insight.

5 [Connect vRealize Operations Manager to vRealize Log Insight for VMware Cloud Foundation in Region A](#)

After the failover of the management applications to Region B and the recovery of the Region A environment, to continue log collection from Region A, reconfigure the vRealize Log Insight Adapter to integrate vRealize Log Insight with vRealize Operations Manager.

Reconfigure the NSX Instance for the Management Cluster for VMware Cloud Foundation in Region A

When Region A is back online after a disaster recovery to Region B, to avoid conflicts in the management and control planes of NSX, modify the roles of the NSX Managers and delete certain NSX components in Region A.

When the NSX instance for the management cluster in Region A is back online, the NSX Manager in Region A still has the primary role. The legacy universal NSX Controller cluster and UDLR control VM in Region A are duplicating the functions of the NSX components that you deployed in Region B during disaster recovery.

Procedure

- 1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Setting	Value
URL	https://sfo01m01vc01.sfo01.rainpole.local/ui
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Networking and security** inventory, click **Installation and upgrade**.

- 3 On the **Management** tab, click the **NSX Managers** tab.

Both NSX Manager instances **172.16.11.65** and **172.17.11.65** are assigned the primary role.

- 4 Remove the NSX Manager instance in Region B as secondary to the NSX Manager instance in Region A.
 - a Select the **172.16.11.65** instance, and, from the **Actions** drop-down menu, select **Remove secondary Manager**.
 - b Select the **Perform operation even if NSX manager is inaccessible** check box and click **Remove**.
- 5 Demote the NSX Manager instance in Region A to the transit role.
 - a Select the **172.16.11.65** instance, and, from the **Actions** drop-down menu, select **Remove primary role**.
 - b In the confirmation dialog box, click **Yes**.
- 6 Delete the NSX Controller nodes in Region A.
 - a On the **Management** tab, click the **NSX Controller nodes** tab.
 - b From the **NSX Manager** drop-down menu, select **172.16.11.65**.
 - c Select the **sfo01m01nsxc01** node and click **Delete**.
 - d On the confirmation dialog box, click **Delete**.
 - e Delete the remaining sfo01m01nsxc02 and sfo01m01nsxc03 NSX Controller nodes.
 - f When you delete the last controller, select the **Proceed to force delete** option.
- 7 Delete the UDLR node in Region A.
 - a In the **Networking and security** inventory, click **NSX Edges**.
 - b From the **NSX Manager** drop-down menu, select **172.16.11.65**
 - c Select the **sfo01m01udlr01** and click **Delete**.
 - d In the **Delete NSX Edge** confirmation dialog box, click **Delete**.
- 8 Assign the NSX Manager instance for the management cluster in Region A as secondary to the NSX Manager instance in Region B.
 - a In the **Networking and security** inventory, click **Installation and upgrade**.
 - b On the **Management** tab, click the **NSX Managers** tab.
 - c Select the primary **172.17.11.65** instance, and from the **Actions** drop-down menu, select **Add secondary Manager**.

- d In the **New secondary Manager** dialog box, configure the settings and click **Add**.

Setting	Value
NSX Manager	172.16.11.65
User Name	admin
Password	<i>mgmtnsx_admin_password</i>
Confirm Password	<i>mgmtnsx_admin_password</i>

- e In the **Thumbprint confirmation** dialog box, click **Accept**.

Disconnect the Application NSX Load Balancer from the SDDC Network for VMware Cloud Foundation in Region A

Because operations management and cloud management applications are failed over to Region B, disconnect the NSX load balancer for the SDDC management applications in Region A. If the load balancer remains connected to the network, the load balancer might receive data for a management application that is failed over to the other region.

Procedure

- 1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Setting	Value
URL	https://sfo01m01vc01.sfo01.rainpole.local/ui
User name	administrator@vsphere.local
Password	<i>vsphere_admin_password</i>

- 2 In the **Networking and security** inventory, click **NSX Edges**.
- 3 From the **NSX Manager** drop-down menu, select **172.16.11.65**.
- 4 Click the edge link of the **sfo01m01lb01** device.
- 5 Click the **Configure** tab and click the **Interfaces** tab.
- 6 Select the **mgmt-vnic-vrealize-edge** vNIC and click **Edit**.
- 7 In the **Edit interface** dialog box, turn off the **Connectivity status** toggle switch to **Disconnected** and click **Save**.

Configure Routing Between Region A and Region B After Failover for VMware Cloud Foundation

When Region A is back online after a disaster recovery to Region B, you must update the routing configuration to restore routing between Region B and Region A and to optimize route selection.

When Region A is back online, on the universal distributed logical router in Region B, you must add a route to the ECMP-enabled NSX Edge nodes in Region A to provide connection to the secondary management components in Region A. You also update the routing configuration in the SDDC to direct traffic to the NSX components in Region B with priority.

Procedure

- 1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Setting	Value
URL	https://sfo01m01vc01.sfo01.rainpole.local/ui
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Networking and security** inventory, click **NSX Edges**.
- 3 Configure BGP on the universal distributed logical router in Region B.
 - a From the **NSX Manager** drop-down menu, select **172.17.11.65**.
 - b Click the edge link of the **sfo01m01udlr01** device.
 - c Click the **Routing** tab and, in the left pane, click **BGP**.
 - d Select the neighbor NSX Edge devices, click **Edit**, configure the following settings, and click **Save**.

Setting	Value for sfo01m01esg01	Value for sfo01m01esg02
IP Address	192.168.10.1	192.168.10.2
Forwarding Address	192.168.10.3	192.168.10.3
Protocol Address	192.168.10.4	192.168.10.4
Remote AS	65003	65003
Weight	10	10
Keep Alive Time	1	1
Hold Down Time	3	3
Password	<i>BGP_password</i>	<i>BGP_password</i>

- e Click **Publish**.
- f In the left pane, click **Static routes**.
- g Select the existing static route (Network: 172.17.11.0/24) and click **Edit**.
- h In the **Edit static route** dialog box, configure the settings and click **Save**.

Setting	Value
Network	172.16.11.0/24
Next Hop	192.168.10.1,192.168.10.2
Admin Distance	1

- i Click **Publish**.

- 4 Reduce the BGP weight of the sfo01m01esg01 and sfo01m01esg02 NSX Edge nodes.
 - a On the **NSX Edges** page, from the **NSX Manager** drop-down menu, select **172.16.11.65**.
 - b Click the edge link of the **sfo01m01esg01** device.
 - c Click the **Routing** tab.
 - d In the left pane, click **BGP**, select the **192.168.10.4** neighbor, and click **Edit**.
 - e In the **Edit BGP neighbor** dialog box, change the **Weight** value to **10** and click **Save**.
 - f Click **Publish**.
 - g Repeat the step for the sfo01m01esg02 edge.
- 5 Verify that the NSX Edge nodes are successfully peering and that BGP routing has been established.
 - a Log in to the first NSX Edge device by using a Secure Shell (SSH) client.

Setting	Value
Hostname	sfo01m01esg01
User name	admin
Password	edge_admin_password

- b To display information about the BGP connections to neighbors, run the `show ip bgp neighbors` command.
The BGP State displays `Established UP` if you have successfully peered with UDLR.
- c To verify that you are receiving routes using BGP, run the `show ip route` command.
- d Repeat the step for the sfo01m01esg02 NSX Edge node.

Restore the Original DNS Record for vRealize Log Insight for VMware Cloud Foundation in Region A

When Region A is back online, update the DNS record for the vRealize Log Insight instance in Region A with the original IP address so that the management applications that are running again in Region A can start sending log data to vRealize Log Insight.

Procedure

- 1 Log in to the DNS server **dc51rp1.rainpole.local** that resides in Region B as an Active Directory administrator by using a Remote Desktop Protocol (RDP) connection.
- 2 Open the Windows **Start** menu, enter **dns** in the **Search** text box, and press Enter.
The **DNS Manager** dialog box appears.
- 3 In the **DNS Manager** dialog box, under **Forward Lookup Zones**, select the **sfo01.rainpole.local** domain by expanding the tree and locate the sfo01vrli01 record on the right side.

- 4 Double-click the **sfo01vrli01** record on the right, change the IP address of the record from **192.168.32.10** to **192.168.31.10**, and click **OK**.

Setting	Value
Fully qualified domain name (FQDN)	sfo01vrli01.sfo01.rainpole.local
IP Address	192.168.31.10
Update associated pointer (PTR) record	Selected

Connect vRealize Operations Manager to vRealize Log Insight for VMware Cloud Foundation in Region A

After the failover of the management applications to Region B and the recovery of the Region A environment, to continue log collection from Region A, reconfigure the vRealize Log Insight Adapter to integrate vRealize Log Insight with vRealize Operations Manager.

Procedure

- 1 In a Web browser, log in to the vRealize Operations Manager by using the operations interface.

Settings	Value
URL	https://vrops01svr01.rainpole.local
User name	admin
Password	<i>vrops_admin_password</i>

- 2 On the main navigation bar, click **Administration**.
- 3 In the left pane, navigate to **Solutions > Configuration**.
- 4 In the **Solutions** section, select **VMware vRealize Log Insight**, and, in the **Configure adapter instances** section, click the **Configure** icon.

The **Manage solution - VMware vRealize Log Insight** dialog box opens.

- 5 In the **Instance settings** pane, modify the settings for the connection to vRealize Log Insight.

Setting	Value
Display Name	Log Insight Adapter - sfo01vrli01
Description	vRealize Log Insight for sfo01
Log Insight server	sfo01vrli01.sfo01.rainpole.local

- 6 To verify that vRealize Operations Manager can connect to vRealize Log Insight, click **Test connection** and in the **Info** dialog box click **OK**.
- 7 Click **Save settings** and in the **Info** dialog box click **OK**.
- 8 In the **Manage solution - VMware vRealize Log Insight** dialog box, click **Close**.

Results

The vRealize Log Insight Adapter is available on the **Solutions** page of the vRealize Operations Manager user interface. The **Collection State** of the adapter is Collecting and the **Collection Status** is Data receiving.

Failback of the SDDC Management Applications for VMware Cloud Foundation

9

Configure and perform a failback of the management applications in the SDDC from the protected region, Region B, to the recovery region, Region A. Failing back these applications restores the pre-recovery configuration of the SDDC.

You fail back the following management components:

- vRealize Suite Lifecycle Manager
- Analytics cluster of vRealize Operations Manager
- Primary components of vRealize Automation with embedded vRealize Orchestrator.

The vSphere Proxy Agents of vRealize Automation is not failed over. Deploy a separate pair of agents in region B in an application isolated network.

- Deployment and configuration of these components are out of scope for this document and must be configured separately.

Table 9-1. Support for Failback of the SDDC Management Components

Management Component	Supports Fail Back
vRealize Suite Lifecycle Manager Appliance	Yes
vRealize Operations Manager analytics nodes	Yes
vSphere Proxy Agents	No
vRealize Automation Appliance	Yes
Microsoft SQL Server	Yes
IaaS Components	Yes

Procedure

1 [Test Failback of the SDDC Management Applications for VMware Cloud Foundation](#)

You can identify potential problems during a future failback by testing the recovery plans for the management applications in the SDDC.

2 [Perform Failback as Planned Migration of the SDDC Management Applications for VMware Cloud Foundation](#)

After you have successfully configured and tested failback of the SDDC management applications and you have restored the infrastructure of Region A, start the migration process from Region B back to Region A.

3 [Perform Failback as Disaster Recovery of the SDDC Management Applications for VMware Cloud Foundation](#)

If Region B becomes unavailable in the event of a disaster, you perform a failback as disaster recovery to Region A by preparing the network and NSX components in Region A, updating the vSAN Default Storage policy, and performing failback of the operations management applications and the Cloud Management Platform.

Test Failback of the SDDC Management Applications for VMware Cloud Foundation

You can identify potential problems during a future failback by testing the recovery plans for the management applications in the SDDC.

- [Test Failback of the Operations Management Applications for VMware Cloud Foundation](#)
Validate the configuration for failback by testing the recovery plan for vRealize Operations Manager and vRealize Suite Lifecycle Manager.
- [Test Failback of the Cloud Management Platform for VMware Cloud Foundation](#)
Validate the configuration for failback of vRealize Automation by testing the recovery plan for the cloud management applications in advance.

Test Failback of the Operations Management Applications for VMware Cloud Foundation

Validate the configuration for failback by testing the recovery plan for vRealize Operations Manager and vRealize Suite Lifecycle Manager.

Site Recovery Manager runs the analytics nodes of vRealize Operations Manager and vRealize Suite Lifecycle Manager on the test network and on a temporary snapshot of replicated data in Region A.

Procedure

- 1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Settings	Value
URL	https://lax01m01vc01.lax01.rainpole.local/ui
User name	administrator@vsphere.local
Password	<i>vsphere_admin_password</i>

- 2 In the **Site Recovery** inventory, on the **lax01m01vc01.lax01.rainpole.local** site pane, click **Open Site Recovery**.

The **Site Recovery** page opens.

- 3 Log in to the VMware Site Recovery Manager user interface by using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

Note Authentication is required if the connection between the protected and the recovery sites has been interrupted after the last successful authentication.

- 4 On the **lax01m01vc01.lax01.rainpole.local** to **sfo01m01vc01.sfo01.rainpole.local** site pair pane, click **View details**.
- 5 On the main navigation bar, click the **Recovery plans** tab and, in the left pane, navigate to **Recovery plans > SDDC Operations Management RP**.
- 6 Click the **Recovery steps** tab, and click the **Test** button.
The **Test - SDDC Operations Management RP** dialog box opens.
- 7 On the **Confirmation options** page, leave the **Replicate recent changes to recovery site** check box selected and click **Next**.
- 8 On the **Ready to complete** page, click **Finish** to initiate the test recovery.
- 9 After the test recovery process finishes, to clean up all the created test virtual machines, click the **Cleanup** button.
The **Cleanup - SDDC Operations Management RP** dialog box opens.
- 10 On the **Confirmation options** page, click **Next**.
- 11 On the **Ready to complete** page, click **Finish**.

After the clean-up process finishes, **Plan status** must be Ready.

Test Failback of the Cloud Management Platform for VMware Cloud Foundation

Validate the configuration for failback of vRealize Automation by testing the recovery plan for the cloud management applications in advance.

Site Recovery Manager runs vRealize Automation virtual machines on the test network and on a temporary snapshot of replicated data in Region A.

Procedure

- 1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Settings	Value
URL	https://lax01m01vc01.lax01.rainpole.local/ui
User name	administrator@vsphere.local
Password	<i>vsphere_admin_password</i>

- 2 In the **Site Recovery** inventory, on the **lax01m01vc01.lax01.rainpole.local** site pane, click **Open Site Recovery**.

The **Site Recovery** page opens.

- 3 Log in to the VMware Site Recovery Manager user interface by using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	<i>vsphere_admin_password</i>

Note Authentication is required if the connection between the protected and the recovery sites has been interrupted after the last successful authentication.

- 4 On the **lax01m01vc01.lax01.rainpole.local** to **sfo01m01vc01.sfo01.rainpole.local** site pair pane, click **View details**.
- 5 On the main navigation bar, click the **Recovery plans** tab and, in the left pane, navigate to **Recovery plans > SDDC Cloud Management RP**.
- 6 Click the **Recovery steps** tab, and click the **Test** button.
The **Test - SDDC Operations Management RP** dialog box opens.
- 7 On the **Confirmation options** page, leave the **Replicate recent changes to recovery site** check box selected and click **Next**.
- 8 On the **Ready to complete** page, click **Finish** to initiate the test recovery.

Note Because recovered virtual machines are using the test network, VMware Tools on the vra01svr01a, vra01svr01b, and vra01svr01c virtual machines might not start within the default timeout. In the recovery plan, increase the startup delay for VMware Tools for these virtual machines to complete the test.

- 9 To resume the recovery plan test, on the **User prompt** dialog box, click **Dismiss**.
- 10 After the test failback process finishes, to clean up all the created test virtual machines, click the **Cleanup** button.

The **Cleanup - SDDC Operations Management RP** dialog box opens.

- 11 On the **Confirmation options** page, click **Next**.

12 On the **Ready to complete** page, click **Finish**.

After the clean-up process finishes, **Plan status** must be Ready.

Perform Failback as Planned Migration of the SDDC Management Applications for VMware Cloud Foundation

After you have successfully configured and tested failback of the SDDC management applications and you have restored the infrastructure of Region A, start the migration process from Region B back to Region A.

- [Initiate Failback as a Planned Migration of the Operations Management Applications for VMware Cloud Foundation](#)

To migrate the virtual machines of the analytics cluster of vRealize Operations Manager and vRealize Suite Lifecycle Manager from Region B back to Region A under planned circumstances, run the recovery plan for the operations management applications from Region B.

- [Initiate Failback as a Planned Migration of the Cloud Management Platform for VMware Cloud Foundation](#)

To migrate the virtual machines of vRealize Automation from Region B to back to Region A under planned circumstances, run the recovery plan for the cloud management applications in Site Recovery Manager from Region B.

Initiate Failback as a Planned Migration of the Operations Management Applications for VMware Cloud Foundation

To migrate the virtual machines of the analytics cluster of vRealize Operations Manager and vRealize Suite Lifecycle Manager from Region B back to Region A under planned circumstances, run the recovery plan for the operations management applications from Region B.

Before failing back the analytics cluster of vRealize Operations Manager, you must take it offline. After the failback operation finishes, you bring the analytics cluster online with the cluster in Region A.

Procedure

1 In a Web browser, log in to the vRealize Operations Manager by using the administration interface.

Settings	Value
URL	https://vrops01svr01a.rainpole.local/admin
User name	admin
Password	<i>vrops_admin_password</i>

- 2 Take the vRealize Operations Manager analytics cluster offline.
 - a In the left pane, click **System status**.
 - b On the **System status** page, under **Cluster status**, click **Take offline**.
 - c In the **Take cluster offline** dialog box, in the **Reason** text box, enter **Planned Migration of the Operations Management applications**, and click **OK**.

Wait until all vRealize Operations Manager nodes are offline and the **Cluster status** becomes **Offline**.

- 3 In a Web browser, log in to vCenter Server by using the vSphere Client.

Settings	Value
URL	https://lax01m01vc01.lax01.rainpole.local/ui
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 4 In the **Site Recovery** inventory, on the **lax01m01vc01.lax01.rainpole.local** site pane, click **Open Site Recovery**.

The **Site Recovery** page opens.

- 5 Log in to the VMware Site Recovery Manager user interface by using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

Note Authentication is required if the connection between the protected and the recovery sites has been interrupted after the last successful authentication.

- 6 On the **lax01m01vc01.lax01.rainpole.local** to **sfo01m01vc01.sfo01.rainpole.local** site pair pane, click **View details**.
- 7 On the main navigation bar, click the **Recovery plans** tab and, in the left pane, navigate to **Recovery plans > SDDC Operations Management RP**.
- 8 To initiate the failback as planned migration of vRealize Operations Manager and vRealize Suite Lifecycle Manager, click the **Recovery steps** tab and click **Run**.

The **Recovery - SDDC Operations Management RP** wizard opens.

- 9 On the **Confirmation options** page, configure the settings for planned migration and click **Next**.

Setting	Value
I understand that this process will permanently alter the virtual machines and infrastructure of both the protected and recovery datacenters.	Selected
Recovery type	Planned migration

10 On the **Ready to complete** page, click **Finish**.

11 In a Web browser, log in to the vRealize Operations Manager by using the administration interface.

Settings	Value
URL	https://vrops01svr01a.rainpole.local/admin
User name	admin
Password	vrops_admin_password

12 Take the vRealize Operations Manager analytics cluster online.

- a In the navigation pane, click **System status**.
- b On the **System status** page, under **Cluster status**, click **Bring online**.

What to do next

- 1 Verify that vRealize Suite Lifecycle Manager is up and operates correctly after a failback. See *Verification of vRealize Suite Lifecycle Manager* in the *VMware Validated Design Operational Verification* documentation.
- 2 Verify that vRealize Operations Manager is up and operates correctly after a failback. See *Verification of vRealize Operations Manager* in the *VMware Validated Design Operational Verification* documentation. If vRealize Operations Manager is not operational, log in to the vRealize Operations Manager master node, take the cluster offline and then bring the cluster back online.
- 3 Prepare vRealize Operations Manager and vRealize Suite Lifecycle Manager for failover by reprotecting the virtual machines of the analytics cluster and the vRealize Suite Lifecycle Manager in Site Recovery Manager. See [Reprotect the Operations Management Applications for VMware Cloud Foundation](#).

Initiate Failback as a Planned Migration of the Cloud Management Platform for VMware Cloud Foundation

To migrate the virtual machines of vRealize Automation from Region B to back to Region A under planned circumstances, run the recovery plan for the cloud management applications in Site Recovery Manager from Region B.

Procedure

1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Settings	Value
URL	https://lax01m01vc01.lax01.rainpole.local/ui
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Site Recovery** inventory, on the **lax01m01vc01.lax01.rainpole.local** site pane, click **Open Site Recovery**.

The **Site Recovery** page opens.

- 3 Log in to the VMware Site Recovery Manager user interface by using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

Note Authentication is required if the connection between the protected and the recovery sites has been interrupted after the last successful authentication.

- 4 On the **lax01m01vc01.lax01.rainpole.local** to **sfo01m01vc01.sfo01.rainpole.local** site pair pane, click **View details**.
- 5 On the main navigation bar, click the **Recovery plans** tab and, in the left pane, navigate to **Recovery plans > SDDC Cloud Management RP**.
- 6 To initiate failback as planned migration of the Cloud Management Platform, click the **Recovery steps** tab and click **Run**.

The **Recovery - SDDC Cloud Management RP** wizard opens.

- 7 On the **Confirmation options** page, configure the settings for planned migration and click **Next**.

Setting	Value
I understand that this process will permanently alter the virtual machines and infrastructure of both the protected and recovery datacenters.	Selected
Recovery type	Planned migration

- 8 On the **Ready to complete** page, click **Finish**.
- 9 During planned migration, execution of the recovery plan pauses after powering on priority 1 virtual machines and priority 2 virtual machines. Perform the steps in KB article [74879](#) and, on the **User prompt** dialog box, click **Dismiss** to resume the planned migration.

What to do next

- 1 Verify that vRealize Automation virtual machines are operational. See *Operational Verification of the Cloud Management Layer* in the *VMware Validated Design Operational Verification* documentation. If vRealize Automation is not operational, restart the vRealize Automation virtual machines. See *SDDC Startup and Shutdown* in the *VMware Validated Design Operational Verification* documentation.
- 2 Prepare vRealize Automation for failover by reprotecting their virtual machines in Site Recovery Manager. See [Reprotect the Cloud Management Platform for VMware Cloud Foundation](#).

Perform Failback as Disaster Recovery of the SDDC Management Applications for VMware Cloud Foundation

If Region B becomes unavailable in the event of a disaster, you perform a failback as disaster recovery to Region A by preparing the network and NSX components in Region A, updating the vSAN Default Storage policy, and performing failback of the operations management applications and the Cloud Management Platform.

Prerequisites

You perform failback as disaster recovery if the following conditions are met:

- The SDDC management applications reside in Region B after a previous failover.
- The SDDC management applications are reprotected from Region B to Region A. See [Reprotect the Operations Management Applications for VMware Cloud Foundation](#) and [Reprotect the Cloud Management Platform for VMware Cloud Foundation](#).

Procedure

1 [Assign the Primary Role to the NSX Manager Instance for the Management Cluster for VMware Cloud Foundation in Region A](#)

If a site failure occurs after you fail over the SDDC management applications to Region B, you must prepare the network layer in Region A for a failback of the management applications. First change the role of the NSX Manager instance in Region A to primary so that you can recreate the virtual network infrastructure in Region A by using NSX Manager.

2 [Redeploy the Control VM of the Universal Distributed Logical Router for VMware Cloud Foundation in Region A](#)

During failover of the SDDC management applications to Region B, the universal NSX components for dynamic routing are deployed in Region B. If a site failure occurs in Region B, the management applications might lose connectivity if you fail them back to Region A right away. Deploy and configure a control VM for the universal dynamic logical router sfo01m01udlr01 in Region A to restore dynamic routing for the management applications.

3 [Reconfigure the Universal Distributed Logical Router and NSX Edge Nodes for Dynamic Routing for VMware Cloud Foundation in Region A](#)

To support dynamic routing in Region A before you initiate disaster recovery from Region B, you configure the universal distributed logical router sfo01m01udlr01, and NSX Edge nodes sfo01m01esg01 and sfo01m01esg02. This configuration ensures that the management components of the SDDC continue to communicate using optimal routes in a fault-tolerant network.

4 [Verify the Establishment of BGP for the Universal Distributed Logical Router for VMware Cloud Foundation in Region A](#)

Verify that the UDLR for the management applications is successfully peering, and that BGP routing has been established in Region A. After you perform failback for disaster recovery, they can continue communicating to keep SDDC operational.

5 [Deploy the NSX Controllers for the NSX Instance for VMware Cloud Foundation in Region A](#)

Deploy the three-node universal NSX Controller cluster in Region A for logical switching and routing in and across the clusters and regions in the SDDC after a failback.

6 [Connect the Application NSX Load Balancer for VMware Cloud Foundation in Region A to the SDDC Network](#)

Enable the network connectivity on sfo01m01lb01 load balancer to support high availability and distribute the network traffic load for the Operations Management applications, and the Cloud Management Platform after failback for disaster recovery to Region A.

7 [Update the vSAN Default Storage Policy of the Management Cluster for VMware Cloud Foundation in Region A](#)

In an environment with multiple availability zones, if a site failure in Region B occurs, the witness appliance in Region B becomes inaccessible. As a result, one fault domain becomes unavailable for the vSAN stretched cluster. To continue provisioning virtual machines in Region A, configure vSAN by using the vSAN default storage policy to force-provision these virtual machines although they will be non-compliant until the witness appliance rejoins Region A. You perform this operation only when multiple availability zones are configured in your environment.

8 [Initiate Disaster Recovery of the Operations Management Applications for VMware Cloud Foundation in Region A](#)

If a site failure in Region B occurs after you failed over the SDDC management applications, initiate disaster recovery of vRealize Suite Lifecycle Manager and of vRealize Operations Manager to keep the monitoring functionality of the SDDC running.

9 [Initiate Disaster Recovery of the Cloud Management Platform for VMware Cloud Foundation in Region A](#)

If a site failure in Region B occurs, initiate a disaster recovery of the vRealize Automation components to keep the workload provisioning functionality of the SDDC available.

10 [Post-Failback Configuration of the SDDC Management Applications for VMware Cloud Foundation](#)

After failback of the Operations Management applications and the Cloud Management Platform, you must perform certain tasks to ensure that applications perform as expected.

11 [Additional Post-Failback Configuration After Region B Is Available Again for VMware Cloud Foundation](#)

When the protected region, Region B, is back online, you can fully transfer all features of the original SDDC configuration to Region A. Integrate the running management nodes in Region B in the main SDDC configuration that is failed back to Region A.

Assign the Primary Role to the NSX Manager Instance for the Management Cluster for VMware Cloud Foundation in Region A

If a site failure occurs after you fail over the SDDC management applications to Region B, you must prepare the network layer in Region A for a failback of the management applications. First change the role of the NSX Manager instance in Region A to primary so that you can recreate the virtual network infrastructure in Region A by using NSX Manager.

Procedure

- 1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Setting	Value
URL	https://sfo01m01vc01.sfo01.rainpole.local/ui
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Networking and security** inventory, click **Installation and upgrade**.
- 3 On the **Management** tab, click the **NSX Managers** tab.
- 4 Disconnect the NSX Manager instance for the management cluster in Region A from the primary NSX Manager instance in Region B.
 - a Select the IP address of the NSX Manager instance for Region A **172.16.11.65**.
 - b From the **Actions** menu, select **Disconnect from Primary NSX Manager**.
 - c In the **Disconnect from Primary NSX Manager** dialog box, click **Yes**.
The operation sets the role of the NSX Manager instance to transit.
- 5 Promote the NSX Manager for the management cluster in Region A to the primary role.
 - a Select the IP address of the NSX Manager instance for Region A **172.16.11.65**.
 - b From the **Actions** menu, select **Assign Primary role**.
 - c In the **Assign Primary role** dialog box, click **Yes**.

Redeploy the Control VM of the Universal Distributed Logical Router for VMware Cloud Foundation in Region A

During failover of the SDDC management applications to Region B, the universal NSX components for dynamic routing are deployed in Region B. If a site failure occurs in Region B, the management applications might lose connectivity if you fail them back to Region A right away. Deploy and configure a control VM for the universal dynamic logical router sfo01m01udlr01 in Region A to restore dynamic routing for the management applications.

Procedure

- 1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Setting	Value
URL	https://sfo01m01vc01.sfo01.rainpole.local/ui
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Networking and security** inventory, click **NSX Edges**.

- 3 From the **NSX Manager** drop-down menu, select **172.16.11.65** .
- 4 Redeploy the control VM of the universal distributed logical router.
 - a Click the edge link of **sfo01m01udlr01**.
 - b Click the **Configure** tab and, in the left pane, click **Appliance settings**.
 - c In the **Edge appliance VMs** section, click the **Add** icon in the edge appliance card.
 - d In the **Add Edge appliance VM** dialog box, configure the settings and click **Add**.

Setting	Value
Data center	sfo01-m01dc
Cluster/Resource Pool	sfo01-m01-mgmt01
Datastore	sfo01-m01-vsan01

- e Repeat this step to deploy a second NSX Edge appliance with the same configuration.
- 5 Configure high availability for the control VMs of the universal distributed logical router.
 - a On the **Configure** tab for sfo01m01udlr01, in the left pane, click **High availability**.
 - b In the to **Management/HA interface** section, click **Edit**, set **Connected to** to **sfo01-m01-vds01-management** and click **Save**.
 - c In the **High availability configuration** section, click **Edit**, configure the settings and click **Save**.

Setting	Value
HA Status	Enable
Declare Dead Time	15
Logging	Enable
Log Level	Info

- 6 Configure the credentials for running commands on the control VMs of the universal logical router.
 - a From the **Actions** menu at the top of the **sfo01m01udlr01** page, select **Change CLI credentials**.
 - b In the **Change CLI credentials** dialog box, configure the settings and click **OK**.

Setting	Value
User Name	admin
Password	<i>udlr_admin_password</i>
Confirm Password	<i>udlr_admin_password</i>

Reconfigure the Universal Distributed Logical Router and NSX Edge Nodes for Dynamic Routing for VMware Cloud Foundation in Region A

To support dynamic routing in Region A before you initiate disaster recovery from Region B, you configure the universal distributed logical router sfo01m01udlr01, and NSX Edge nodes sfo01m01esg01 and sfo01m01esg02. This configuration ensures that the management components of the SDDC continue to communicate using optimal routes in a fault-tolerant network.

Procedure

- 1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Setting	Value
URL	https://sfo01m01vc01.sfo01.rainpole.local/ui
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Networking and security** inventory, click **NSX Edges**.
- 3 From the **NSX Manager** drop-down menu, select **172.16.11.65**.
- 4 Verify the routing configuration for the universal distributed logical router.
 - a Click the edge link of **sfo01m01udlr01**.
 - b Click the **Routing** tab and verify the settings.

Setting	Value
Global Configuration > Routing Configuration > ECMP	Started
Global Configuration > Dynamic Routing Configuration > Router ID	192.168.10.3

- 5 To verify the protocol settings and configure BGP peering between the UDLR device and the NSX Edge nodes for the ECMP-enabled North-South routing in Region A, on the left side, select **BGP**.
 - a Verify the settings.

Setting	Value
Status	Started
Local AS	65003
Graceful Restart	Started

- b Under **Neighbors**, select **192.168.10.1** and click the **Edit** icon.

The **192.168.10.1** entry represents the connection settings for the sfo01m01esg01 neighbor.

- c In the **Edit BGP Neighbor** dialog box, update the **Weight** value to **60**, enter the BGP password that was configured during the initial setup of the UDLR, and click **Save**.

Setting	sfo01m01esg01 Value	sfo01m01esg02 Value
IP Address	192.168.10.1	192.168.10.2
Forwarding Address	192.168.10.3	192.168.10.3
Protocol Address	192.168.10.4	192.168.10.4
Remote AS	65003	65003
Weight	60	60
Keep Alive Time	1	1
Hold Down Time	3	3
Password	<i>BGP_password</i>	<i>BGP_password</i>

- d On the **BGP** page, repeat the steps for the **192.168.10.2** entry which represents the sfo01m01esg02 neighbor.
- e Click **Publish**.

- 6 On the left side, select **Route Redistribution** to verify redistribution status.

Category	Setting	Value
Route Redistribution Status	OSPF	Deselected
	BGP	Selected
Route Redistribution table	Learner	BGP
	From	Connected
	Prefix	Any
	Action	Permit

- 7 Reconfigure the routing and weight value of sfo01m01esg01 and sfo01m01esg02 edge devices.
- a In the **Navigator**, click **NSX Edges**.
- b Select **172.16.11.65** from the **NSX Manager** drop-down menu.
- c Click the edge link of **sfo01m01esg01** to open its configuration interface.
- d Click the **Routing** tab.
- e On the left side, select **BGP**, select the **192.168.10.4** neighbor, and click **Edit**.
- f In the **Edit Neighbor** dialog box, change the **Weight** value to **60** and click **Save**.
- g Click **Publish**.
- h Repeat this step for the sfo01m01esg02 edge.

Verify the Establishment of BGP for the Universal Distributed Logical Router for VMware Cloud Foundation in Region A

Verify that the UDLR for the management applications is successfully peering, and that BGP routing has been established in Region A. After you perform failback for disaster recovery, they can continue communicating to keep SDDC operational.

Procedure

- 1 Log in to the Universal Distributed Logical Router by using a Secure Shell (SSH) client.

Setting	Value
Hostname	sfo01m01udlr01
User name	admin
Password	<i>udlr_admin_password</i>

- 2 Verify that the UDLR can peer with the ECMP-enabled NSX Edge services gateways.
 - a To display information about the BGP and TCP connections to the UDLR neighbors, run the `show ip bgp neighbors` command.
 - b In the command output, verify that the BGP state is `Established`, up for 192.168.10.1 (sfo01m01esg01) and 192.168.10.2 (sfo01m01esg02).
- 3 Verify that the UDLR receives routes by using BGP and that multiple routes are established to BGP-learned networks.
 - a Run the `show ip route` command.
 - b In the command output, verify that the routes to the networks are marked with the letter B and several routes to each adjacent network exist.

The letter B in front of each route indicates that the route is established over BGP.

Deploy the NSX Controllers for the NSX Instance for VMware Cloud Foundation in Region A

Deploy the three-node universal NSX Controller cluster in Region A for logical switching and routing in and across the clusters and regions in the SDDC after a failback.

Procedure

- 1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Setting	Value
URL	https://sfo01m01vc01.sfo01.rainpole.local/ui
User name	administrator@vsphere.local
Password	<i>vsphere_admin_password</i>

2 Deploy the universal controller cluster in Region A.

You deploy three NSX Controller nodes with the same configuration.

- a In the **Networking and security** inventory, click **Installation and upgrade**.
- b On the **Management** tab, click the **NSX Controller nodes** tab.
- c From the **NSX Manager** drop-down menu, select **172.16.11.65**.
- d Under **Controller Nodes**, click the **Add** icon.
- e If you deploy the first NSX Controller node, in the **Add Controller** dialog box, configure the settings and click **Next**.

Setting	Value
Password	<i>mgmtnsx_controllers_password</i>
Confirm Password	<i>mgmtnsx_controllers_password</i>

- f In the **Deployment & connectivity** dialog box, configure the settings and click **Finish**.

Setting	Value
Name	<ul style="list-style-type: none"> ■ sfo01m01nsrc01 for the first NSX Controller ■ sfo01m01nsrc02 for the second NSX Controller ■ sfo01m01nsrc03 for the third NSX Controller
Datacenter	sfo01-m01dc
Cluster/Resource Pool	sfo01-m01-mgmt01
Datastore	sfo01-m01-vsan01
Folder	sfo01-m01fd-nsx
Connected To	sfo01-m01-vds01-management
IP Pool	sfo01-mgmt01-nsrc01

- g After the **Status** of the controller node that you are deploying changes to **Connected**, deploy the remaining two NSX Controller nodes sfo01m01nsrc02 and sfo01m01nsrc03.

3 Synchronize the state of the newly deployed controllers by using the Update Controller State mechanism on the NSX Manager instance in Region B.

An Update Controller State operation pushes the current VXLAN and universal distributed logical router configuration from NSX Manager to the NSX Controller cluster.

- a In the **Networking and security** inventory, click **Installation and Upgrade**.
- b On the **Management** tab, click the **NSX Managers** tab and select the **172.16.11.65** instance.
- c From the **Actions** drop-down menu, select **Update Controller state**.
- d In the **Update Controller state** dialog box, click **Yes**.

- 4 Configure DRS anti-affinity rule for the deployed NSX Controller nodes.
 - a In the **Hosts and clusters** inventory, expand the **sfo01m01vc01.sfo01.rainpole.local** tree and expand the **sfo01-m01dc** data center.
 - b Select the **sfo01-m01-mgmt01** cluster.
 - c Click the **Configure** tab and under **Configuration**, select **VM/Host rules**.
 - d To create an anti-affinity rule, in the **VM/Host rules** list, click **Add**.
 - e In the **Create VM/Host Rule** dialog box, configure the settings and click **OK**.

Setting	Value
Name	anti-affinity-rule-nsxc
Enable rule	Selected
Type	Separate Virtual Machines
Members	<ul style="list-style-type: none"> ■ sfo01m01nsxc01 ■ sfo01m01nsxc02 ■ sfo01m01nsxc03

Connect the Application NSX Load Balancer for VMware Cloud Foundation in Region A to the SDDC Network

Enable the network connectivity on sfo01m01lb01 load balancer to support high availability and distribute the network traffic load for the Operations Management applications, and the Cloud Management Platform after failback for disaster recovery to Region A.

Procedure

- 1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Setting	Value
URL	https://sfo01m01vc01.sfo01.rainpole.local/ui
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Networking and security** inventory, click **NSX Edges**.
- 3 From the **NSX Manager** drop-down menu, select **172.16.11.65**.
- 4 Click the edge link of **sfo01m01lb01** device.
- 5 Click the **Configure** tab.
- 6 Click **Interfaces**, select the **mgmt-vnic-vrealize-edge** vNIC, and click **Edit**.
- 7 In the **Edit interface** dialog box, set **Connectivity Status** to **Connected** and click **Save**.

Update the vSAN Default Storage Policy of the Management Cluster for VMware Cloud Foundation in Region A

In an environment with multiple availability zones, if a site failure in Region B occurs, the witness appliance in Region B becomes inaccessible. As a result, one fault domain becomes unavailable for the vSAN stretched cluster. To continue provisioning virtual machines in Region A, configure vSAN by using the vSAN default storage policy to force-provision these virtual machines although they will be non-compliant until the witness appliance rejoins Region A. You perform this operation only when multiple availability zones are configured in your environment.

Procedure

- 1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Setting	Value
URL	https://sfo01m01vc01.sfo01.rainpole.local/ui
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Policies and profile** inventory, click **VM storage policies**.
- 3 On the **VM storage policies** page, select the **vSAN default storage policy** for management vCenter Server and click **Edit settings**.
The **Edit VM storage policy** wizard opens.
- 4 On the **Name and description** page, leave the default values and click **Next**.
- 5 On the **vSAN** page, click the **Advanced policy rules** tab, turn on the **Force provisioning** toggle switch and click **Next**.
- 6 On the **Storage compatibility** page, leave the default values and click **Next**.
- 7 On the **Review and finish** page, click **Finish**.
VM Storage Policy in Use dialog box appears.
- 8 In the **vSAN Storage Policy in Use** dialog box, from the **Reapply to VMs** drop-down menu, select **Manually later** and click **Yes**.

Initiate Disaster Recovery of the Operations Management Applications for VMware Cloud Foundation in Region A

If a site failure in Region B occurs after you failed over the SDDC management applications, initiate disaster recovery of vRealize Suite Lifecycle Manager and of vRealize Operations Manager to keep the monitoring functionality of the SDDC running.

Procedure

- 1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Setting	Value
URL	https://sfo01m01vc01.sfo01.rainpole.local/ui
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Site Recovery** inventory, on the **sfo01m01vc01.sfo01.rainpole.local** site pane, click **Open Site Recovery**.

The **Site Recovery** page opens.

- 3 Log in to the VMware Site Recovery Manager user interface by using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

Note Authentication is required if the connection between the protected and the recovery sites has been interrupted after the last successful authentication.

- 4 On the **sfo01m01vc01.sfo01.rainpole.local** to **lax01m01vc01.lax01.rainpole.local** site pair pane, click **View details**.
- 5 On the main navigation bar, click the **Recovery plans** tab and, in the left pane, navigate to **Recovery plans > SDDC Operations Management RP**.
- 6 To initiate the failback of vRealize Operations Manager and vRealize Suite Lifecycle Manager, click the **Recovery steps** tab and click **Run**.

The **Recovery - SDDC Operations Management RP** wizard opens.

- 7 On the **Confirmation options** page, configure the settings for disaster recovery and click **Next**.

Setting	Value
I understand that this process will permanently alter the virtual machines and infrastructure of both the protected and recovery datacenters.	Selected
Recovery type	Disaster recovery

- 8 On the **Ready to complete** page, click **Finish**.

What to do next

- 1 Verify that vRealize Suite Lifecycle Manager is operational correctly after a failback. See *Verification of vRealize Suite Lifecycle Manager* in the *VMware Validated Design Operational Verification* documentation.

- 2 Verify that vRealize Operations Manager is operational after the failback. See *Verification of vRealize Operations Manager* in the *VMware Validated Design Operational Verification* documentation. If vRealize Operations Manager is not operational, log in to the vRealize Operations Manager master node, take the cluster offline and then bring the cluster back online.
- 3 Complete the configuration of the SDDC in Region A. See [Post-Failback Configuration of the SDDC Management Applications for VMware Cloud Foundation](#).
- 4 Prepare vRealize Operations Manager and vRealize Suite Lifecycle Manager for failover by reprotecting the virtual machines of the analytics cluster and the vRealize Suite Lifecycle Manager in Site Recovery Manager. See [Reprotect the Operations Management Applications for VMware Cloud Foundation](#).

Initiate Disaster Recovery of the Cloud Management Platform for VMware Cloud Foundation in Region A

If a site failure in Region B occurs, initiate a disaster recovery of the vRealize Automation components to keep the workload provisioning functionality of the SDDC available.

Procedure

- 1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Setting	Value
URL	https://sfo01m01vc01.sfo01.rainpole.local/ui
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Site Recovery** inventory, on the **sfo01m01vc01.sfo01.rainpole.local** site pane, click **Open Site Recovery**.

The **Site Recovery** page opens.

- 3 Log in to the VMware Site Recovery Manager user interface by using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

Note Authentication is required if the connection between the protected and the recovery sites has been interrupted after the last successful authentication.

- 4 On the **sfo01m01vc01.sfo01.rainpole.local** to **lax01m01vc01.lax01.rainpole.local** site pair pane, click **View details**.
- 5 On the main navigation bar, click the **Recovery plans** tab and, in the left pane, navigate to **Recovery plans > SDDC Cloud Management RP**.

- To initiate the failback of the Cloud Management Platform, click the **Recovery steps** tab and click **Run**.

The **Recovery - SDDC Cloud Management RP** wizard opens.

- On the **Confirmation options** page, configure the settings for planned migration and click **Next**.

Setting	Value
I understand that this process will permanently alter the virtual machines and infrastructure of both the protected and recovery datacenters.	Selected
Recovery type	Disaster recovery

- On the **Ready to complete** page, click **Finish**.
- During disaster recovery, execution of the recovery plan pauses after powering on priority 1 virtual machines and priority 2 virtual machines. Perform the steps in KB article [74879](#) and, on the **User prompt** dialog box, click **Dismiss** to resume the planned migration.

What to do next

- Verify that vRealize Automation virtual machines are operational. See *Operational Verification of the Cloud Management Layer* in the *VMware Validated Design Operational Verification* documentation. If vRealize Automation is not operational, restart the vRealize Automation virtual machines. See *SDDC Startup and Shutdown* in the *VMware Validated Design Operational Verification* documentation.
- Complete the SDDC configuration in Region A. See [Post-Failback Configuration of the SDDC Management Applications for VMware Cloud Foundation](#).
- Prepare vRealize Automation for failover by reprotecting their virtual machines in Site Recovery Manager. See [Reprotect the Cloud Management Platform for VMware Cloud Foundation](#).

Post-Failback Configuration of the SDDC Management Applications for VMware Cloud Foundation

After failback of the Operations Management applications and the Cloud Management Platform, you must perform certain tasks to ensure that applications perform as expected.

Procedure

- [Revert the vSAN Default Storage Policy of the Management Cluster for VMware Cloud Foundation in Region A](#)

In an environment with multiple availability zones, change the vSAN default storage policy of the management cluster in Region A back to its original configuration after the SDDC failback is complete. In this way, vSAN can provision management virtual machines by using the stretched cluster capabilities again. You perform this operation only when multiple availability zones are configured in your environment.

2 Configure the UDLR Control Virtual Machine to Forward Events to vRealize Log Insight for VMware Cloud Foundation in Region A

Configure the UDLR control VM instances for the management cluster to forward log information to vRealize Log Insight in Region A.

Revert the vSAN Default Storage Policy of the Management Cluster for VMware Cloud Foundation in Region A

In an environment with multiple availability zones, change the vSAN default storage policy of the management cluster in Region A back to its original configuration after the SDDC failback is complete. In this way, vSAN can provision management virtual machines by using the stretched cluster capabilities again. You perform this operation only when multiple availability zones are configured in your environment.

Procedure

- 1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Setting	Value
URL	https://sfo01m01vc01.sfo01.rainpole.local/ui
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Policies and profile** inventory, click **VM storage policies**.
- 3 On the **VM storage policies** page, select the **vSAN default storage policy** and click **Edit settings**.
The **Edit VM storage policy** wizard opens.
- 4 On the **Name and description** page, leave the default values and click **Next**.
- 5 On the **vSAN** page, click the **Advanced policy rules** tab, turn off the **Force provisioning** toggle switch and click **Next**.
- 6 On the **Storage compatibility** page, leave the default values and click **Next**.
- 7 On the **Review and finish** page, click **Finish**.
VM Storage Policy in Use dialog box appears.
- 8 In the **vSAN Storage Policy in Use** dialog box, from the **Reapply to VMs** drop-down menu, select **Manually later** and click **Yes**.

During this operation, vSAN performance might be affected as objects are recreated to match the storage policy.

Configure the UDLR Control Virtual Machine to Forward Events to vRealize Log Insight for VMware Cloud Foundation in Region A

Configure the UDLR control VM instances for the management cluster to forward log information to vRealize Log Insight in Region A.

Procedure

- 1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Setting	Value
URL	https://sfo01m01vc01.sfo01.rainpole.local/ui
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Networking and security** inventory, click **NSX Edges**.
- 3 Configure the newly deployed control VM of the UDLR in Region A to forward events to vRealize Log Insight in Region A.
 - a From the **NSX Manager** drop-down menu, select **172.16.11.65**.
 - b Click the edge link of **sfo01m01udlr01** device.
 - c Click the **Configure** tab and, in the left pane, click **Appliance settings**.
 - d Click the **Configuration** icon and select **Change syslog configuration**.
 - e In the **Change syslog servers** dialog box, configure the settings and click **OK**.

Setting	Value
Server 1	192.168.31.10
Protocol	UDP

Additional Post-Failback Configuration After Region B Is Available Again for VMware Cloud Foundation

When the protected region, Region B, is back online, you can fully transfer all features of the original SDDC configuration to Region A. Integrate the running management nodes in Region B in the main SDDC configuration that is failed back to Region A.

Procedure

- 1 [Reconfigure the NSX Instance for the Management Cluster for VMware Cloud Foundation in Region B](#)

When Region B is back online after a failback for disaster recovery to Region A, to avoid conflicts in the management and control planes of NSX, modify the roles of the NSX Managers and delete certain NSX components in Region B.

- 2 [Disconnect the Application NSX Load Balancer from the SDDC Network for VMware Cloud Foundation in Region B](#)

Because operations management and cloud management applications are failed back to Region A, disconnect the NSX load balancer for the SDDC management applications in Region B from the network. If the load balancer remains connected to the network, the load balancer might receive data for a management application that is already failed backed to the other region.

3 Revert the Routing Configuration Between Region A and Region B After Failback for VMware Cloud Foundation

When Region B is back online after a disaster recovery to Region A, you must update the routing configuration to implement the original routing setup between Region B and Region A.

Reconfigure the NSX Instance for the Management Cluster for VMware Cloud Foundation in Region B

When Region B is back online after a failback for disaster recovery to Region A, to avoid conflicts in the management and control planes of NSX, modify the roles of the NSX Managers and delete certain NSX components in Region B.

When the NSX instance for the management cluster in Region B is back online, the NSX Manager instance in Region B still has the primary role. The legacy universal NSX Controller cluster and UDLR control VM in Region B are duplicating the functions of the NSX components that you deployed in Region A during the failback for disaster recovery.

Procedure

- 1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Settings	Value
URL	https://lax01m01vc01.lax01.rainpole.local/ui
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Networking and security** inventory, click **Installation and upgrade**.
- 3 On the **Management** tab, click the **NSX Managers** tab.

Both NSX Manager instances **172.16.11.65** and **172.17.11.65** are assigned the primary role.
- 4 Remove the NSX Manager instance in Region A as secondary to the NSX Manager instance in Region B.
 - a Select the **172.17.11.65** instance, and from the **Actions** drop-down menu, select **Remove secondary Manager**.
 - b Select the **Perform operation even if NSX manager is inaccessible** check box and click **Remove**.
- 5 Demote the NSX Manager instance in Region B to the transit role.
 - a Select the **172.17.11.65** instance, from the **Actions** drop-down menu, select **Remove primary role**.
 - b In the confirmation dialog box, click **Yes**.
- 6 Delete the NSX Controller nodes in Region B.
 - a On the **Management** tab, click the **NSX Controller nodes** tab.
 - b From the **NSX Manager** drop-down menu, select **172.17.11.65**.

- c Select the **lax01m01nsrc01** node and click **Delete**.
 - d On the confirmation dialog box, click **Delete**.
 - e Delete the remaining lax01m01nsrc02 and lax01m01nsrc03 NSX Controller nodes.
 - f When you delete the last controller, select the **Proceed to force delete** option .
- 7 Delete the UDLR node in Region B.
- a In the **Networking and security** inventory, click **NSX Edges**.
 - b From the **NSX Manager** drop-down menu, select **172.17.11.65**
 - c Select **sfo01m01udlr01** and click **Delete**.
 - d In the **Delete NSX Edge** confirmation dialog box, click **Delete**.
- 8 Assign the NSX Manager instance for the management cluster in Region B as secondary to the NSX Manager instance in Region A.
- a In the **Networking and security** inventory, click **Installation and upgrade**.
 - b On the **Management** tab, click the **NSX Managers** tab.
 - c Select the primary **172.16.11.65** instance, and from the **Actions** drop-down menu, select **Add secondary Manager**.
 - d In the **New secondary Manager** dialog box, configure the settings and click **Add**.

Setting	Value
NSX Manager	172.17.11.65
User Name	admin
Password	<i>mgmtnsx_admin_password</i>
Confirm Password	<i>mgmtnsx_admin_password</i>

- e In the **Thumbprint confirmation** dialog box, click **Accept**.

Disconnect the Application NSX Load Balancer from the SDDC Network for VMware Cloud Foundation in Region B

Because operations management and cloud management applications are failed back to Region A, disconnect the NSX load balancer for the SDDC management applications in Region B from the network. If the load balancer remains connected to the network, the load balancer might receive data for a management application that is already failed backed to the other region.

Procedure

- 1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Setting	Value
URL	https://sfo01m01vc01.sfo01.rainpole.local/ui
User name	administrator@vsphere.local
Password	<i>vsphere_admin_password</i>

- 2 In the **Networking and security** inventory, click **NSX Edges**.
- 3 From the **NSX Manager** drop-down menu, select **172.17.11.65**.
- 4 Click the edge link of the **lax01m01lb01** device.
- 5 Click the **Configure** tab and click the **Interfaces** tab.
- 6 Select the **mgmt-vnic-vrealize-edge** vNIC and click **Edit**.
- 7 In the **Edit interface** dialog box, turn off the **Connectivity status** toggle switch to **Disconnected** and click **Save**.

Revert the Routing Configuration Between Region A and Region B After Failback for VMware Cloud Foundation

When Region B is back online after a disaster recovery to Region A, you must update the routing configuration to implement the original routing setup between Region B and Region A.

When Region B is back online, on the universal distributed logical router in Region A, you must add a route to the ECMP-enabled NSX Edge nodes in Region B to provide connection to the secondary management components in Region B. Also update the routing configuration in the SDDC to direct traffic to the NSX components in Region A with priority.

Procedure

- 1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Setting	Value
URL	https://sfo01m01vc01.sfo01.rainpole.local/ui
User name	administrator@vsphere.local
Password	<i>vsphere_admin_password</i>

- 2 In the **Networking and security** inventory, click **NSX Edges**.
- 3 Configure BGP on the universal distributed logical router in Region B.
 - a From the **NSX Manager** drop-down menu, select **172.16.11.65**.
 - b Click the edge link of the **sfo01m01udlr01** device.
 - c Click the **Routing** tab and, in the left pane, click **BGP**.

- d Select the neighbor NSX Edge devices, click **Edit**, configure the settings, and click **Save**.

Setting	lax01m01esg01 Value	lax01m01esg02 Value
IP Address	192.168.10.50	192.168.10.51
Forwarding Address	192.168.10.3	192.168.10.3
Protocol Address	192.168.10.4	192.168.10.4
Remote AS	65003	65003
Weight	10	10
Keep Alive Time	1	1
Hold Down Time	3	3
Password	<i>BGP_password</i>	<i>BGP_password</i>

- e Click **Publish**.
- f In the left pane, click **Static routes**.
- g Select the existing static route (Network: 172.16.11.0/24) and click **Edit**.
- h In the **Edit static route** dialog box, configure the settings and click **Save**.

Setting	Value
Network	172.17.11.0/24
Next Hop	192.168.10.50,192.168.10.51
Admin Distance	1

- i Click **Publish**.
- 4 Reduce the BGP weight of the lax01m01esg01 and lax01m01esg02 NSX Edge nodes.
- a On the **NSX Edges** page, from the **NSX Manager** drop-down menu, select **172.17.11.65**.
- b Click the edge link of the **lax01m01esg01** device.
- c Click the **Routing** tab.
- d In the left pane, click **BGP**, select the **192.168.10.4** neighbor, and click **Edit**.
- e In the **Edit BGP neighbor** dialog box, change the **Weight** value to **10** and click **Save**.
- f Click **Publish**.
- g Repeat the step for the lax01m01esg02 edge.

5 Verify that the NSX Edge nodes are successfully peering and that BGP routing has been established.

- a Log in to the first NSX Edge device by using a Secure Shell (SSH) client.

Setting	Value
Hostname	lax01m01esg01
User name	admin
Password	<i>edge_admin_password</i>

- b To display information about the BGP connections to neighbors, run the `show ip bgp neighbors` command.

The BGP State displays `Established UP` if you have successfully peered with UDLR.

- c To verify that you are receiving routes using BGP, run the `show ip route` command.
- d Repeat the step for the lax01m01esg02 NSX Edge node.

Reprotect of the SDDC Management Applications for VMware Cloud Foundation

10

After a disaster recovery or planned migration, the recovery region becomes the protected region, but the VMs are not protected yet. If the original protected region is operational, you can reverse the direction of protection to protect the new primary region.

During the reprotect operation, after Site Recovery Manager reverses the direction of protection, it forces a synchronization of the storage from the new protected region to the new recovery region. Forcing data synchronization ensures that the recovery region has a current copy of the protected virtual machines running at the protection region. Recovery is possible immediately after the reprotect operation finishes.

- [Prerequisites for Performing Reprotect for VMware Cloud Foundation](#)

To reprotect the virtual machines of the SDDC management applications, your environment must meet certain requirements for the availability of the original protected region and state of the recovery plans.

- [Reprotect the Operations Management Applications for VMware Cloud Foundation](#)

After the inaccessible region is back online, prepare vRealize Operations Manager and vRealize Suite Lifecycle Manager for failback or failover by reprotecting the virtual machines in Site Recovery Manager.

- [Reprotect the Cloud Management Platform for VMware Cloud Foundation](#)

After the inaccessible region is back online, prepare vRealize Automation for failback or failover by reprotecting the virtual machines in Site Recovery Manager.

Prerequisites for Performing Reprotect for VMware Cloud Foundation

To reprotect the virtual machines of the SDDC management applications, your environment must meet certain requirements for the availability of the original protected region and state of the recovery plans.

- The original protected region must be available. The vCenter Server instances, ESXi hosts, Site Recovery Manager Server instances, and corresponding databases must all be recovered.

To unpair and recreate the pairing of protected and recovery regions, both regions must be available. If you cannot restore the original protected region, you must reinstall Site Recovery Manager on the protected and recovery regions.

- If you performed a planned migration or disaster recovery, verify that all steps of the recovery plan finish successfully. If errors occur during the recovery, resolve the problems that caused the errors and rerun the recovery plan. When you rerun a recovery plan, the operations that previously succeeded are skipped. For example, successfully recovered virtual machines are not recovered again and continue running without interruption.
- If you performed a disaster recovery operation, you must perform the following tasks before reprotect:
 - After the protected region is repaired, Site Recovery Manager detects the availability of the region and changes the status of the recovery plan to *Recovery Required*. Rerun the recovery plans for the Cloud Management Platform and operations management applications in the *Recovery Required* state so that Site Recovery Manager can perform actions on the original region which failed during disaster recovery.
 - Perform a planned migration when both regions are running again.
If errors occur during the planned migration, resolve the errors and rerun the planned migration until it succeeds.

Reprotect the Operations Management Applications for VMware Cloud Foundation

After the inaccessible region is back online, prepare vRealize Operations Manager and vRealize Suite Lifecycle Manager for failback or failover by reprotecting the virtual machines in Site Recovery Manager.

Procedure

- 1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Setting	Value
URL for reprotect after failover.	<code>https://lax01m01vc01.lax01.rainpole.local/ui</code>
URL for reprotect after failback.	<code>https://sfo01m01vc01.sfo01.rainpole.local/ui</code>
User name	<code>administrator@vsphere.local</code>
Password	<code>vsphere_admin_password</code>

- 2 In the **Site Recovery** inventory, on the **lax01m01vc01.lax01.rainpole.local** site pane, click **Open Site Recovery**.

The **Site Recovery** page opens.

3 Log in to the VMware Site Recovery Manager user interface by using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

Note Authentication is required if the connection between the protected and the recovery sites has been interrupted after the last successful authentication.

- 4 On the **lax01m01vc01.lax01.rainpole.local** to **sfo01m01vc01.sfo01.rainpole.local** site pair pane, click **View details**.
- 5 On the main navigation bar, click the **Recovery plans** tab and, in the left pane, navigate to **Recovery plans > SDDC Operations Management RP**.
- 6 Right-click the **SDDC Operations Management RP** recovery plan, and select **Reprotect**.
The **Reprotect - SDDC Operations Management RP** wizard opens.
- 7 On the **Confirmation options** page, select the check box confirming that you understand the reprotect operation is irreversible, and click **Next**.
- 8 On the **Ready to complete** page, review the reprotect information and click **Finish**.
- 9 To monitor the progress of the reprotect, click the **SDDC Operations Management RP** recovery plan and on the **SDDC Operations Management RP** page, click the **Recovery Steps** tab.
- 10 If the status of the SDDC Operations Management RP recovery plan changes to Reprotect interrupted, open the **Reprotect - SDDC Operations Management RP** wizard again and select the **Force cleanup** check box on the confirmation page.
- 11 After the status of the SDDC Operations Management RP recovery plan changes to Ready, click the **History** tab and click **Export All**.
- 12 Verify that the history report contains no errors
The recovery plan can return to the Ready state even if errors occurred during the reprotect operation.
- 13 If errors occurred during the reprotect operation, resolve them and run a test recovery to verify that the errors are fixed.
If you skip resolving the errors and attempt to run a planned migration or disaster recovery later, the recovery of some virtual machines might fail.

Results

After reprotect, Site Recovery Manager performs the following actions:

- Reverses the recovery site and protected site.
- Creates placeholder copies of the virtual machines of vRealize Operations Manager and vRealize Suite Lifecycle Manager from the new protected site to the new recovery site.

Reprotect the Cloud Management Platform for VMware Cloud Foundation

After the inaccessible region is back online, prepare vRealize Automation for failback or failover by reprotecting the virtual machines in Site Recovery Manager.

Procedure

- 1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Setting	Value
URL for reprotect after failover.	https://lax01m01vc01.lax01.rainpole.local/ui
URL for reprotect after failback.	https://sfo01m01vc01.sfo01.rainpole.local/ui
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Site Recovery** inventory, on the **lax01m01vc01.lax01.rainpole.local** site pane, click **Open Site Recovery**.

The **Site Recovery** page opens.

- 3 Log in to the VMware Site Recovery Manager user interface by using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

Note Authentication is required if the connection between the protected and the recovery sites has been interrupted after the last successful authentication.

- 4 On the **lax01m01vc01.lax01.rainpole.local** to **sfo01m01vc01.sfo01.rainpole.local** site pair pane, click **View details**.
- 5 On the main navigation bar, click the **Recovery plans** tab and, in the left pane, navigate to **Recovery plans > SDDC Cloud Management RP**.
- 6 Right-click the **SDDC Cloud Management RP** recovery plan, and select **Reprotect**.
The **Reprotect - SDDC Cloud Management RP** wizard appears.
- 7 On the **Confirmation options** page, select the check box for confirming that you understand the reprotect operation is irreversible, and click **Next**.
- 8 On the **Ready to complete** page, review the reprotect information and click **Finish**.
- 9 To monitor the progress of the reprotect, click the **SDDC Cloud Management RP** recovery plan and on the **SDDC Cloud Management RP** page, click the **Recovery Steps** tab.

10 If the status of the SDDC Cloud Management RP recovery plan changes to Reprotect interrupted, open the **Reprotect** wizard again and select the **Force cleanup** check box on the confirmation page.

11 After the status of the SDDC Cloud Management RP recovery plan changes to Ready, click the **History** tab and click **Export all**.

12 Verify that the history report contains no errors

The recovery plan can return to the Ready state even if errors occurred during the reprotect operation.

13 If errors occurred during the reprotect operation, resolve them and run a test recovery to verify that the errors are fixed.

If you skip resolving the errors and attempt to run a planned migration or disaster recovery later, the recovery of some virtual machines might fail.

Results

After successful reprotect, Site Recovery Manager performs the following actions:

- Reverses the recovery site and protected site.
- Creates placeholder copies of the virtual machines of the Cloud Management Platform from the new protected site to the new recovery site.